ABSTRACT ALGEBRA

HOLDEN DAY SERIES IN MATHEMATICS

EARL E CODDINGTON and ANDREW M GLEASON *Editors*

Introductory Calculus
S Bell J R Blum J V Lewis and J Rosenblatt

Modern University Calculus
S Bell J R Blum J V Lewis and J Rosenblatt

Elementary Partial Differential Equations
P W Berg and J L McGregor

The Structure of Lie Groups
G Hochschild

Abstract Algebra
A Lindstrum Jr

Set Theory for the Mathematician
J Rubin

Elements of General Topology
Sze Tsen Hu

Elements of Modern Algebra
Sze Tsen Hu

Elements of Real Analysis
Sze Tsen Hu

Introduction to Contemporary Mathematics
Sze Tsen Hu

Introduction to General Topology
Sze Tsen Hu

Homology Theory
Sze Tsen Hu

ABSTRACT ALGEBRA

Andrew O. Lindstrum, Jr.

SOUTHERN ILLINOIS UNIVERSITY
AT EDWARDSVILLE

Library of Congress Catalog Card Number 67 13835
Printed in the United States of America

Preface

My aim in writing this book was to present a logical development of the fundamentals of Abstract Algebra. I have endeavored to avoid assuming anything not proved prior to its use, and particularly to avoid illustrative examples from other parts of mathematics and elsewhere.

Such examples are often more confusing to the student than they are helpful since the student frequently is not acquainted sufficiently with the other material to appreciate, or in many instances, even to *understand* the examples. So far as I can recall at the moment of writing, I have deviated from this policy in only two instances: in some exercises giving groups as rotations of the equilateral triangle and the square, and in taking up briefly, in Chapter 5, the trisection of the angle. These two instances may very well be omitted without interfering with the continuity of the development.

As to the subject matter chosen, I hope that I have chosen the topics most essential to prepare the student for further reading in more specialized books on particular parts of algebra. I should mention that I have been most influenced by the early chapters on *Algèbre* by the great French mathematician, N. Bourbaki, and have generally followed the terminology used there. In recent years there have appeared many individual books devoted to Linear Algebra. A foundation for this subject, given from the point of view of the rest of the book, appears as Chapter 7.

The text is intended for use by the advanced undergraduate or the beginning graduate student. I have attempted to make the text self-contained, but some mathematical maturity is undoubtedly essential to success in mastering the material. The book starts at a relatively elementary level in discussing sets and mappings, and proceeds logically from there. No attempt is made to put the beginnings on a completely postulational basis, such as giving a completely axiomatic treatment of sets; also, no attempt is made to consider the ultimate in simplicity in that no systems with fewer properties than semigroups are treated.

Many of the theorems are left as exercises for the reader These are such that the method of proof is very much like one or more of the theorems proved in the text material or else simple consequences of those theorems Numerous hints are given in the exercises for aiding the student in proving such theorems

Logical symbols are used whenever appropriate such as in stating and proving theorems stating definitions etc I have found considerable difference of feeling on such use A decided majority of mathematicians I have consulted on the matter definitely prefer this method particularly among younger mathematicians It must be admitted that feeling was strong on both sides I have attempted to use such symbols somewhat sparingly at first often stating theorems etc both in words and in symbols giving the reader an opportunity to become familiar with them I feel and most of the mathematicians consulted agree with me that the use of logical symbols results in brevity and much greater clarity

The symbol ■ is used throughout the book to indicate the end of a proof This is due to Prof Paul R Halmos and replaces the older Q E D

The material contained here is somewhat more than the author has found possible to cover in an academic year with even rather superior students This should enable a teacher using this book as a text to choose somewhat among the subjects considered and have enough to occupy a full year course In recent years I have covered very little of Chapter 7 but practically everything in the first six chapters

I have used four earlier versions in multilithed form in teaching year courses in the subject In each revision I have attempted to remove difficulties which the students encountered in the previous version I am thus indebted to many former students for their constructive criticism and their discovery of many errors

I wish to express my appreciation to the Consulting Editor Prof Andrew M Gleason of Harvard and to my colleague Prof Clellie C Oursler for a number of helpful suggestions for improving the manuscript Also I wish to thank my colleagues Prof Oursler and Prof George V Poynor for reading the printer s proofs and making useful comments on the final version of the book

A O Lindstrum Jr

A Short Introduction for the Student

One of the most important problems in the history of mathematics has been the solving of equations, and a very great part of algebra has been devoted to solving equations of two types: (1) single polynomial equations of degree n in one unknown, and (2) linear equations in several unknowns. The first six chapters of the present book are primarily devoted to equations of the first type, culminating in the Galois Theory of Equations. The last chapter and certain parts of the earlier chapters deal with equations of the second type.

It is usually the case in mathematics that continued attempts to solve a particular problem give rise to many more problems with many and various results. This is certainly the case with the attempts to solve equations.

One of these results has been an intensive study of the way in which elements combine under various laws of combining, such as addition, multiplication, and so forth. This has led to an investigation of such fundamental building blocks as sets and mappings. By using mappings of one set into another and defining laws of composition by means of such mappings, it is possible to prove many things more simply and more generally than was possible before. We consider this particularly in the first two chapters.

Another way of studying and obtaining general results is to consider rather uncomplicated systems. We do this in Chapters 1 and 2 when we consider semigroups and groups. By studying such systems we obtain results which apply, for example, to both addition and multiplication and also to many other methods of combining elements.

There are three very important mathematical systems which are very convenient to have available as soon as possible. These are the systems of the natural numbers, the integers, and the rational numbers. We derive these as quickly as is practicable, using the general abstract results which we have been developing. Their derivation, at least that of the integers and the rational numbers, is such as to be applicable to the derivation of other systems.

In Chapter 4 we proceed systematically to develop more and more complicated mathematical systems having more and more laws of composition As we proceed we consider the most important properties of these systems

In Chapters 5 and 6 we are particularly interested in that abstract system whose prototype is the set of rational numbers It is the system called a field It is of particular significance for the solution of equations since one important problem is to determine for a polynomial equation of degree *n* when it is possible to find a formula involving addition subtraction multiplication division and the extraction of roots performed on the coefficients of the equation which will give the roots of the equation A field is the most general system in which addition subtraction multiplication and division (except by zero) can always be carried out Many of the results of group theory are found to be useful in considering fields *The culmination of our study* of fields is contained in the theorems of the Galois Theory of Fields

A problem in mathematics can be disposed of in either of two ways by giving its solution or by proving that there is no solution The problem of finding a formula of the type described in the above paragraph is disposed of in the Galois Theory of Equations by the proof that such a formula cannot exist if the degree of the equation is 5 or greater We conclude Chapter 6 by considering the Galois Theory of Equations

In Chapter 7 we complete our study of the problem of the second type given at the start of this Introduction and proceed to an extensive discussion of various concepts which arose in the process of disposing of this problem

So far we have been considering how the solution of equations has been studied However it often happens in mathematics that the methods developed to solve one problem or a set of problems are found to be of importance and benefit in other parts of mathematics This has definitely been the case with our present subject Most of the methods and concepts which are developed in this book have wide application both in algebra and in other branches of mathematics This is why we spend as much time as we do in making precise and detailed investigation of so many different concepts If our purpose were only the solution of the two types of equations given at the beginning we could accomplish it in much less time and space

In accord with present practices in mathematics the method of *presentation is abstract and formal Once the reader has grown* accustomed to it he should find this clearer and more concise than other methods

Contents

Chapter 1: Sets, Mappings, Laws of Composition, and Natural Numbers

In this chapter we begin with a presentation of certain notation and symbols which we shall use throughout the book. Then we discuss sets, mappings, and set products and use them to define laws of internal composition. Next we consider various fundamental properties which may be possessed by such laws. Finally, we end the chapter with a development of a mathematical system of the utmost importance, the natural numbers.

1. LOGIC

We shall assume a knowledge of ordinary logic. In giving mathematical proofs and in making mathematical statements in general, it is often necessary to say, "if statement A holds, then statement B holds." It is briefer to say, "statement A implies statement B," or briefer yet to say, "A implies B," where we have let the letter A represent one statement and the letter B another. We then proceed one step further and introduce a symbol for the word "implies," listing it and several other useful logical symbols below.

The symbol $\Rightarrow$ means "implies" or "imply," depending on the context. Thus we write $A \Rightarrow B$, and read it, "A implies B."

The symbol $\Leftrightarrow$ means, when placed between two statements, that each statement implies the other. Thus it can be interpreted to mean, "if and only if." Thus $A \Leftrightarrow B$ can be read, "A implies B and is implied by B," or, "A if and only if B." So this means that A is a necessary and sufficient condition for B, and B is a necessary and sufficient condition for A.

The symbol $\ni$ means "such that."

The symbol $\exists$ means "there exists" or "there exist," depending on the context.

The symbol $\forall$ means "for all," "for every," or "for each," depending on the context.

The symbol / when written through another symbol means the negation of the statement in which the second symbol occurs Thus $\nexists$ means there does not exist or there do not exist depending on the context

Since the reader may not be familiar with the use of these logical symbols we shall use them somewhat sparingly at first and we shall often give statements twice once in symbolic form and then written out in words (or in the reverse order)

We shall use equality of two objects is meaning identity and thus we have the following properties in which the letters a b c represent any objects with which we may deal

E_R $a = a$ the *reflexive* property
E_S If $a = b$ then $b = a$ the *symmetric* property
E_T If $a = b$ and $b = c$ then $a = c$ the *transitive* property

These last two properties can be written using symbols as follows

E_S $(a = b) \Rightarrow (b = a)$ $\qquad$ E_T $(a = b$ and $b = c) \Rightarrow (a = c)$

2 SETS

We shall not attempt to give a definition of a set Usually it will be sufficient for the determination of a set A to have a criterion by which to determine whether or not a particular object x belongs to A We may on occasion use the terms *collection grouping* as synonyms for set We shall say that a set consists of elements or objects

In giving a set S we may write $S = \{a\ b\ c\ d \qquad \}$ and mean that S consists of the objects a b c which are listed within the braces or if $\phi(x)$ is the condition (or the conditions) which an element x of S must satisfy in order to belong to S we may write $S = \{x|\phi(x)\}$ and by this mean that S consists of all objects x which satisfy the condition $\phi(x)$

DEFINITION 2 1 $\quad a \in A$ if and only if a is an element of the set A [In symbols $(a \in A) \Leftrightarrow a$ is an element of the set A This is read a belongs to A or sometimes a belonging to A]

$A \subset B$ where A and B are sets if and only if whenever $a \in A$ then $a \in B$ (This is read A is contained in B which means that every element of A is an element of B)

$A \supset B$ if and only if $B \subset A$

A is a *subset* of B if and only if $A \subset B$

A is a *proper subset* of B if and only if $A \subset B$ and $A \neq B$

$\varnothing$ denotes the *empty* (or *null*) set. (That is, $\varnothing$ is the set containing no elements.)

PROBLEM 2.1. Prove that if A and B are any two sets, then $A = B$ if and only if $A \subset B$ and $B \subset A$.

In Problems 2.2 and 2.3 and in Problems 3.1 through 3.5 we shall consider the following particular sets: $D = \{a, b, c, d\}$, $E = \{a, b, d\}$, $F = \{a, d, e, f\}$, $G = \{d, e, f, g\}$, $U = \{a, b, c, d, e, f, g\}$.

PROBLEM 2.2. Find all subsets of the sets D and E. (Do not forget $\varnothing$.)

DEFINITION 2.2. Let A and B be any subsets of a set S. Then $A \cup B$ is the set of all elements belonging to A, to B, or to both. It is called the *union* of A and B. $A \cap B$ is the set of all elements belonging both to A and to B. It is called the *intersection* or *common part* of A and B. The sets A and B are called *disjoint* if and only if $A \cap B = \varnothing$.

PROBLEM 2.3. Find $D \cup E$, $D \cap E$, $D \cap F$, $D \cap G$.

PROBLEM 2.4. Express $A \cup B$ and $A \cap B$ in the form immediately preceding Definition 2.1.

3. MAPPING OF ONE SET INTO ANOTHER

DEFINITION 3.1. A *mapping*, α, of a set, S, *into* a set, T, is defined whenever to each element $s \in S$, there is associated with it exactly one element $t \in T$. The element, t, is called the *image* of s and we usually denote it by $s\alpha = t$, or, to use functional notation, $\alpha(s) = t$. The mapping itself is sometimes written as $\alpha: S \rightarrow T$. The set of all elements of T which are images under α of elements of S is called the *set of images of S under* α, and is denoted by $S\alpha$.

The reader should observe that the same element of the set T may be the image of several different elements of S. Thus, α is a mapping of the set D into the set E as defined immediately above Problem 2.2, if $a\alpha = a$, $b\alpha = a$, $c\alpha = b$, $d\alpha = d$. Here $a \in T$ is the image of both $a \in S$ and $b \in S$.

Not all the elements of the set T need to be images of elements of S. Thus β is a mapping of E into F (above Problem 2.2) if $a\beta = a$, $b\beta = d$, $d\beta = e$. Here f is not the image of any element of S (which here is E).

However, γ defined by $a\gamma = a$, $b\gamma = b$, $d\gamma = d$ is *not* a mapping of D into E, since there is no image given for the element $c \in D$.

DEFINITION 3.2. If α and β are mappings of the set S into the set T, then $\alpha = \beta$ if and only if for all $s \in S$ the image under α is the same as the image under β. [In symbols: $(\alpha = \beta) \Leftrightarrow (\forall s \in S, s\alpha = s\beta)$.]

In the particular mapping β given above, we observed that not all elements of F were images of elements of E. It is convenient to have a particular name for mappings of S into T in which all elements of T are images. Also, in the mapping α above, $a \in E$ was the image of two elements $a, b \in D$. Here also it is convenient to have a particular name for mappings which do not have this property, that is, *for mappings of S into T in which no element of T is the image of more than one element of S*.

DEFINITION 3.3. Let α be a mapping of the set S into the set T. Then we have

(a) α is a mapping of S *onto* T if and only if each element of T is the image of some element of S.

(b) α is a 1-1 mapping (read "one to one") of S into T if and only if no two elements of S have the same image in T.

It should be noted that S and T may be the same set, say S. Then we refer to mappings of S into S as *mappings of S into itself* (or *onto itself*).

PROBLEM 3.1. Which of the following mappings of D into F are 1-1? Which are onto? (a) $a\delta = d$, $b\delta = c$, $c\delta = d$, $d\delta = a$. (b) $a\theta = e$, $b\theta = f$, $c\theta = a$, $d\theta = d$. (c) $a\phi = e$, $b\phi = e$, $c\phi = e$, $d\phi = e$. (D and F as of §2.)

PROBLEM 3.2. (a) Show that if $a\iota = a$, $b\iota = b$, $c\iota = c$, $d\iota = d$, then ι is a 1-1 mapping of D onto itself. (b) Show that if for an arbitrary set S, $\forall s \in S$, $s\iota = s$, then ι is a 1-1 mapping of S onto itself. This mapping is called the *identity mapping* of S onto itself.

PROBLEM 3.3. Show that there does not exist a 1-1 mapping of D onto E. Generalize.

Sometimes we are interested only in how a mapping of S into T affects a particular subset of S. And, going in the opposite direction, we may have a mapping of a subset S_1 of S into a subset T_1 of T and we may wish to extend this mapping to get a mapping of S into T. We now introduce terminology for these cases.

DEFINITION 3.4. Let S_1, T_1 be subsets of the sets S and T respectively.

(a) Let α be a mapping of S into T. Then α_1, defined by $(\forall s_1 \in S_1, s_1\alpha_1 = t \Leftrightarrow s_1\alpha = t)$, is called the *restriction of* α *to* S_1.

(b) Let α be a mapping of S_1 into T_1. Then a mapping, β, of S into T is an *extension of* α *to* $S \Leftrightarrow (\forall s \in S_1, s\alpha = s\beta)$.

PROBLEM 3.4. Let $H = \{a, b\}$. Give the restriction to H of the mapping of D into E immediately following Definition 3.1.

PROBLEM 3.5. After the manner of Definition 3.2 give three different extensions of β (introduced immediately following Definition 3.1.) to D.

4. SET PRODUCTS AND LAWS OF COMPOSITION

DEFINITION 4.1. Let α be a mapping of the set I into the set A and let $\iota\alpha = a_\iota$, $\forall \iota \in I$. Then $\{a_\iota\}_{\iota\in I}$ is the set of all images under this mapping α. If I consists of all elements $i \in N \ni i \leq n \in N$, then the set of images is usually denoted by $\{a_i\}_{i=1,2,\ldots,n}$ or $\{a_1, a_2, \ldots, a_n\}$. (For definition of N, see Section 6 below.)

Thus $\{a_i\}_{i=1,2,3}$ denotes the set of three elements $\{a_1, a_2, a_3\}$.

DEFINITION 4.2. The *set product* of a family of sets $\{E_\iota\}_{\iota\in I}$ (cf. Definition 4.1), denoted by $\Pi_{\iota\in I}\, E_\iota$, is the set of all sets $\{x_\iota | x_\iota \in E_\iota\}_{\iota\in I}$. This set product is often called the *Cartesian product* of the family of sets.

As in Definition 4.1, the set I, called the *indexing set*, can be any set. One very important such set is $I = \{1, 2\}$. Letting $E_1 = S$ and $E_2 = T$, we may say that the set product of S and T, denoted by $S \times T$, is the set of all ordered pairs, (x, y), where $x \in S$ and $y \in T$.

PROBLEM 4.1. Let $H = \{a, b, c\}$, $K = \{d, e\}$. Give all the elements of $H \times K$. How many distinct elements are there?

PROBLEM 4.2. For H as in Problem 4.1, find $H \times H$, and determine the number of distinct elements.

The reader has, in his previous experience, encountered such processes as addition, multiplication, subtraction, division, exponentiation, etc. These processes are such that given two numbers in a specified order, there is assigned to them, except in a few special cases, another number. We wish to give an abstract formulation of this, and do so in the next definition.

DEFINITION 4.3. A *law of internal composition* between elements of a set S, is a mapping of a part A of $S \times S$ into S. For a particular element $(s_1, s_2) \in A$, the image under this mapping is called the *composite of s_1 and s_2* under this law. If $A = S \times S$, the law is said to be *defined everywhere* and the set S is said to be *closed* with respect to (or under) this law of composition. (Sometimes if $A = S \times S$, such a law is called a binary operation.)

EXAMPLE 4.1. Let $K = \{d, e\}$ and let α be the following mapping of $K \times K$ into K: $(d, d)\alpha = d$, $(d, e)\alpha = e$, $(e, d)\alpha = d$, $(e, e)\alpha = e$. Usually the composite of two elements is represented by using a symbol for the law, placed between the two elements. Thus in this case, if we use $\bigcirc$ to denote the law of composition determined by α, we have $d \bigcirc d = d$, $d \bigcirc e = e$, $e \bigcirc d = d$, $e \bigcirc e = e$.

EXAMPLE 4.2. Another law of composition for K is determined by the mapping β as follows: $(d, d)\beta = e$, $(d, e)\beta = d$, $(e, d)\beta = d$, $(e, e)\beta = e$. By Definition 3.2, these mappings α and β are different. If we denote the composite under β by $\square$, we have $d \square d = e$, $d \square e = d$, $e \square d = d$, $e \square e = e$.

EXAMPLE 4.3. A law of composition for $H = \{a, b, c\}$ is determined by the mapping γ as follows: $(a, a)\gamma = b$, $(a, b)\gamma = c$, $(b, a)\gamma = c$, $(a, c)\gamma = b$, $(c, a)\gamma = b$, $(b, c)\gamma = a$, $(c, b)\gamma = a$, $(b, b)\gamma = a$, $(c, c)\gamma = c$. Thus if we let $\triangle$ denote the law of composition determined by γ, we have $a \triangle a = b$, $a \triangle b = b \triangle a = c$, $a \triangle c = a \triangle c = b$, $b \triangle c = c \triangle b = a$, $c \triangle c = c$.

PROBLEM 4.3. Give two other laws of composition defined everywhere in the above set K.

PROBLEM 4.4. Give another law of composition defined everywhere in the above set H.

PROBLEM 4.5. Let U be as defined previously (following Problem 2.1) and let P be the set of all subsets of U. Verify in a few cases that union and intersection are both laws of internal composition defined everywhere in P.

PROBLEM 4.6. Let U be any set and let P be the set of all subsets of U. Prove that $\cup$ and $\cap$ are laws of internal composition defined everywhere in P.

5 PROPERTIES OF LAWS OF INTERNAL COMPOSITION

COMMUTATIVITY. The reader has probably noticed that in Example 4.1 $d \bigcirc e = e$ while $e \bigcirc d = d$. Thus the order of the two elements in the composite is of considerable importance. Often, however, the order does not matter, and, in that case, we have a special name to describe the law.

Definition 5.1. If $\Box$ is a law of internal composition defined in a set S and if, whenever $a \Box b$ is defined, for $a, b \in S$, $a \Box b = b \Box a$, then and only then the law $\Box$ is called *commutative.*

Problem 5.1. Examine the laws of Examples 4.2 and 4.3 and those you gave in Problems 4.3 and 4.4 for commutativity.

Problem 5.2. Prove that $\cup$ and $\cap$ are both commutative (cf. Problem 4.6).

Associativity. As we have defined a law of composition, we can apparently only find the composite of two elements. If we write, purely formally, $a \Box b \Box c$ for an arbitrary law $\Box$ of internal composition, this expression as it stands is meaningless. We could, however, find the composite of a and b, let it be d, and then find the composite of d and c. Or we could find the composite of b and c, let it be e, and then find the composite of a and e. That is, we form the composite of two adjacent elements and then the composite of that with the third. It is customary to use some sort of grouping symbols, such as parentheses, brackets, braces, etc., to indicate which composite is to be found first. The one to be found first is always the one enclosed by the parentheses or other such symbols. Thus we write the two cases discussed above as $(a \Box b) \Box c$ and $a \Box (b \Box c)$, respectively. The reader is undoubtedly familiar with the statement that these last two expressions are equal. This is not always the case and we use a special name to describe the law involved when it is.

Definition 5.2. If $\Box$ is a law of internal composition defined in a set S and if, whenever $(a \Box b) \Box c$ and $a \Box (b \Box c)$ are both defined, $a, b, c \in S$, we have $(a \Box b) \Box c = a \Box (b \Box c)$, then and only then is the law $\Box$ called *associative.*

To test whether or not a law is associative requires considering the equation in Definition 5.2 for all possible choices of a, b, c. In general, this may be rather difficult or, in some cases, not difficult but quite tedious. For instance, in Example 4.3, there are 27 cases to be considered. For the other examples in the same paragraph, only eight cases are present.

Problem 5.3. Determine whether or not the law of Example 4.1 is associative.

PROBLEM 5 4 Prove that $\cup$ and $\cap$ are associative

DISTRIBUTIVITY The reader is familiar from his previous mathematical experience with sets in which two or more laws of internal composition are defined We have already had a few such examples such as the sets H and K of Section 4 Also $\cup$ and $\cap$ are two different laws of composition defined everywhere in the set of all subsets of a given set It is natural to consider relations between two or more such laws Probably the most important such relationship is that considered in the next definition

DEFINITION 5 3 If $\square$ and $\bigcirc$ are two laws of internal composition defined in a set S and if whenever $a \,\square\, (b \bigcirc c)$ and $(a \,\square\, b) \bigcirc (a \,\square\, c)$ are both defined in S a b $c \in S$ $a \,\square\, (b \bigcirc c) = (a \,\square\, b) \bigcirc (a \,\square\, c)$ then and only then is the law $\square$ called *left distributive with respect to* $\bigcirc$

In a similar manner we can define right distributivity by starting with $(b \bigcirc c) \,\square\, a$ (This is left as a problem)

If $\square$ is commutative then $\square$ is left distributive with respect to $\bigcirc$ if and only if $\square$ is right distributive with respect to $\bigcirc$ Then we may say merely distributive

PROBLEM 5 5 Give the full definition of right distributivity of $\square$ with respect to $\bigcirc$

PROBLEM 5 6 State the conditions for right and left distributivity of $\bigcirc$ with respect to $\square$

PROBLEM 5 7 Determine whether or not either of the laws of Examples 4 1 and 4 2 is distributive with respect to the other

PROBLEM 5 8 Prove that $\cup$ is distributive with respect to $\cap$ and that $\cap$ is distributive with respect to $\cup$

6 THE NATURAL NUMBERS

There is one particular mathematical system of such fundamental importance that it becomes very inconvenient and cumbersome to attempt to proceed much further without having it available for our use Accordingly we shall now develop this system and its most important properties Occasionally we shall interrupt this development to consider some general concepts

DEFINITION 6 1 The set N is the set of all natural numbers $\Leftrightarrow$
(1) $\exists\, 1 \in N$

(2) $a \in N$ has a unique *successor*, $a^+ \in N$. The element a is called the *antecedent* of a^+.

(3) 1 has no antecedent

(4) $(a, b \in N, a^+ = b^+) \Rightarrow (a = b)$

(5) if M is a subset of N with the following properties: (i) $1 \in M$; (ii) whenever $a \in M$, then $a^+ \in M$; then $M = N$.

The conditions given in Definition 6.1 are called Peano's Axioms or Peano's Postulates. Condition (5) is called the Axiom of Mathematical Induction, or merely the Induction Axiom.

Presently we are going to define two laws of internal composition in the set N and prove various important properties of these laws. In doing so, since this is a particular set, we shall use extensively the particular properties it possesses. First, however, we prove a result whose proof is very easy. To help the reader understand it, we point out that the theorem implies that the only element of N which does not have an antecedent is the element 1, and that the proof uses Axiom (5). The set M used in the proof is slightly unusual but is of a type occasionally useful.

THEOREM 6.1. $(x \in N, x \neq 1) \Rightarrow (\exists\, y \in N \ni x = y^+)$.

PROOF: Let $M = \{x \mid x \in N \text{ and } (x = 1 \text{ or } \exists\, y \in N \ni x = y^+)\}$. Then by definition of M, $1 \in M$. Now let $x \in M$; then $x^+ \in M$ since x^+ is the successor of x. Hence, whenever $x \in M$, then $x^+ \in M$. Therefore, by Axiom 5, $M = N$. ■

PROBLEM 6.1. Prove that $\forall\, a \in N$, $a^+ \neq a$. [Hint: consider $(a^+)^+$.]

7. ADDITION OF NATURAL NUMBERS

The method used in giving the next definition is often called definition by induction or by recursion. We define the concept for the natural number 1. Then, for each natural number x for which the concept has already been defined, we define it for x^+. The reader might refer back to Definitions 3.1, 4.1, 4.2, and Theorem 6.1 to verify that what we do does define a law of internal composition in N.

DEFINITION 7.1. (Definition of Addition of Natural Numbers) $a, b \in N \Rightarrow$

(1) $a + 1 = a^+$,

(2) $a + b^+ = (a + b)^+$.

THEOREM 7.1. N is closed under addition.

PROOF. By Definition 4.2 we must show that the mapping of Definition 7.1 is a mapping of $N \times N$ into N. Let $a \in N$. If we can show that $\forall b \in N$, $a + b$ is defined and $a + b \in N$, we shall have proved the theorem.

Let $M = \{b | b \in N,\ a + b \text{ is defined and } a + b \in N\}$. By (1) of Definition 7.1, $1 \in M$ since $a + 1 = a^+ \in N$. Let $b \in M$, i.e., $a + b \in N$. Then by (2) of Definition 7.1, $a + b^+ = (a + b)^+ \in N$. Therefore $(b \in M) \Rightarrow (b^+ \in M)$. Therefore by Axiom (5), $N = M$. ■

THEOREM 7.2. Addition in N is associative.

PROOF. Let $a, b \in N$. If we can show that $\forall c \in N$, $(a + b) + c = a + (b + c)$, we shall have established the theorem.

Let $M = \{c | c \in N \text{ and } (a + b) + c = a + (b + c)\}$. Now $(a + b) + 1 = (a + b)^+ = a + b^+ = a + (b + 1)$. Therefore $1 \in M$. Now let $c \in M$, i.e., $(a + b) + c = a + (b + c)$. Then $(a + b) + c^+ = [(a + b) + c]^+ = a + (b + c)^+ = a + (b + c^+) \Rightarrow c^+ \in M$. Therefore $(c \in M) \Rightarrow (c^+ \in M)$. Therefore $M = N$. ■

THEOREM 7.3. Addition in N is commutative.

PROBLEM 7.1. Prove Theorem 7.3. (Hint: first prove by induction on a that $a + 1 = 1 + a$, then use this as the first step in the induction on b to prove that $a + b = b + a$.)

PROBLEM 7.2. Prove that $(a, b \in N) \Rightarrow (a \neq a + b)$.

8. THE CANCELLATION LAW

We now consider another example.

EXAMPLE 8.1. A law of composition for the set $L = \{a, b, c\}$ is defined by the mapping $\forall x, y \in L$, $(x, y)\delta = a$. If we denote this law by ∇, we have $x \nabla y = a$, $\forall x, y \in L$. The law ∇ is obviously commutative and associative, and we have in particular $a \nabla b = a$, $a \nabla c = a$. That is, $a \nabla b = a \nabla c$ but $b \neq c$. This is not the case with most laws of composition with which the reader has had previous acquaintance. The more familiar case is the one covered in the next definition.

DEFINITION 8.1. Let $\square$ be a law of internal composition defined in a set S. Then the *left cancellation law for* $\square$ *holds for the element* $a \in S \Leftrightarrow [\forall x, y \in S,\ (a \square x = a \square y) \Rightarrow (x = y)]$.

In a similar manner we can define the right cancellation law. If both right and left cancellation laws hold, then we say simply that the cancellation law holds. Of course, if □ is commutative, the one will hold if and only if the other does.

PROBLEM 8.1. Examine whether or not the cancellation laws hold for the examples in Section 4.

PROBLEM 8.2. Give another example in which a cancellation law does not hold.

THEOREM 8.1. The cancellation law holds for addition and all elements of N.

PROOF: We must show that $\forall\, a, b, c \in N,\ a + c = b + c \Rightarrow a = b$.

Let $M = \{c | c \in N \text{ and } (\forall\, a, b \in N,\ a + c = b + c \Rightarrow a = b)\}$. Then $1 \in M$, since $a + 1 = a^+$ and $b + 1 = b^+$ by Definition 7.1 and $a^+ = b^+ \Rightarrow a = b$ by Axiom 4 of Definition 6.1.

Let $c \in M$, and let $a + c^+ = b + c^+$. Then $a + (c + 1) = b + (c + 1)$, by Definition 7.1. So, $(a + c) + 1 = (b + c) + 1$ by Theorem 7.2; therefore, since $1 \in M$, $a + c = b + c$. Hence, since $c \in M$, $a = b$. Thus $a + c^+ = b + c^+ \Rightarrow a = b$. Therefore, $c^+ \in M$ whenever $c \in M$. Therefore, $M = N$. ■

PROBLEM 8.3. Prove, without using Theorem 8.1, that $\forall\, a, b, c \in N,\ a \neq b \Rightarrow a + c \neq b + c$.

PROBLEM 8.4. Prove that Theorem 8.1 is equivalent to the statement of Problem 8.3.

THEOREM 8.2. (Law of Trichotomy for N.) $a, b \in \mathrm{N} \Rightarrow$ exactly one of the following statements holds:

(1) $a = b$
(2) $\exists\, c \in N \ni a = b + c$
(3) $\exists\, d \in N \ni b = a + d$.

PROOF: First we establish that no two of these can hold simultaneously. By Problem 7.2, statements (1) and (2) cannot hold simultaneously, nor can statements (1) and (3). If statements (2) and (3) did hold, then we should have $b = (b + c) + d = b + (c + d)$, which is impossible (again by Problem 7.2). Therefore, no more than one of these three cases can hold for two elements $a, b \in N$.

Now we shall show that one case is always present. Let $a \in N$ and let $M = \{b | b \in N$ and one of the three cases holds for a and $b\}$.

Either $a = 1$, or if $a \neq 1$, then by Theorem 6.1 $\exists\, c \in N \ni a = c^+$, i.e., $a = 1 + c$. Thus either case (1) or (2) is present for $b = 1$. Therefore $1 \in M$.

Now let $b \in M$. Then one of the three cases holds for a, b. We shall consider each in turn and show that one of the three cases must hold for a and b^+.

(1) $a = b$. Then $a^+ = b^+$, i.e., $b^+ = a + 1$. So case (3) holds for a and b^+.

(2) $\exists\, c \in N \ni a = b + c$. We have two subcases to consider. If $c = 1$, then $a = b + 1 = b^+$, so we have case (1) for a and b^+. If $c \neq 1$, then by Theorem 6.1 $\exists\, e \in N \ni c = e^+ = 1 + e$, so we have $a = b + (1 + e) = (b + 1) + e = b^+ + e$ and we have case (2) for a and b.

(3) $\exists\, d \in N \ni b = a + d$. Then $b^+ = (a + d)^+ = (a + d) + 1 = a + (d + 1)$, and so we have case (3) for a and b^+. Therefore $b \in M \Rightarrow b^+ \in M$. Therefore $M = N$. ■

9. MULTIPLICATION OF NATURAL NUMBERS

Definition 9.1 (Definition of Multiplication of Natural Numbers) $a, b \in N \Rightarrow$

(1) $a \cdot 1 = a$.

(2) $a \cdot b^+ = (a \cdot b) + a$.

We shall frequently omit the symbol $\cdot$ and understand that if two elements of N are written adjacent to each other they are to be multiplied. Further, if an expression involves both addition and multiplication, it is understood that if there are no parentheses or other symbols of inclusion the multiplications are to be performed before the additions. Thus we write the last expression in Definition 9.1 as $ab + a$.

Theorem 9.1 N is closed under multiplication.

Problem 9.1 Prove Theorem 9.1 (cf. proof of Theorem 7.1).

Theorem 9.2 The Left Distributive Law of Multiplication with respect to Addition holds in N.

Proof By Definition 5.3, we must show that $\forall\, a, b, c \in N$, $a \cdot (b + c) = ab + ac$.

Let $a, b \in N$ and let $M = \{c \mid c \in N \text{ and } a(b + c) = ab + ac\}$. Now $a(b + 1) = ab^+ = ab + a = a \cdot b + a \cdot 1$. Therefore $1 \in M$. Now let $c \in M$. Then $a(b + c^+) = a(b + c)^+ = a(b + c) + a = (ab + ac) + a = ab + (ac + a) = ab + ac^+$. Therefore $c \in M \Rightarrow c^+ \in M$. Therefore $M = N$. ■

THEOREM 9.3. Multiplication in N is associative.

PROBLEM 9.2. Prove Theorem 9.3. [Hint: to prove $(ab)c = a(bc)$, use induction on c, and in considering $(ab)c^+$, use Theorem 9.2.]

LEMMA: $a, b \in N \Rightarrow 1 \cdot a = a$ and $b^+ \cdot a = b \cdot a + a$.

PROBLEM 9.3. Prove the above Lemma. (Hint: use induction on a.)

THEOREM 9.4. Multiplication in N is commutative.

COROLLARY: The Right Distributive Law of Multiplication with respect to Addition holds in N.

PROBLEM 9.4. Prove Theorem 9.4. (Hint: use the Lemma.)

PROBLEM 9.5. Prove the Corollary to Theorem 9.4 directly by using the method of the proof of Theorem 9.2.

10. RELATIONS

We are now going to give a precise definition of what is meant abstractly by a relation. Two such relations are equality and inequality.

DEFINITION 10.1. A *relation* R defined in a set S is a subset R of $S \times S$. We shall write $aRb \Leftrightarrow (a, b) \in R$.

DEFINITION 10.2. (Properties possessed by some relations.) Let R be a relation defined in a set S. Then

(a) R is *reflexive* $\Leftrightarrow \forall\, a \in S$, aRa
(b) R is *symmetric* $\Leftrightarrow (aRb \Rightarrow bRa)$
(c) R is *transitive* $\Leftrightarrow (aRb$ and $bRc \Rightarrow aRc)$.

EXAMPLE 10.1. Let $K = \{d, e\}$. Then if $R = \{(d, d), (e, e)\}$, R is ordinary equality.

EXAMPLE 10.2. Let $K = \{d, e\}$. Then if $R = \{(d, e), (e, d)\}$, R is symmetric, but not reflexive or transitive.

EXAMPLE 10.3. Let $K = \{d, e\}$. Then if $R = \{(e, e)\}$, R is symmetric and transitive, but not reflexive.

DEFINITION 10.3. Let $\square$ be a law of internal composition defined in a set S, and R a relation defined in S. Then R is *left compatible with* $\square \Leftrightarrow a, b \in S$, $\forall\, c \in S$, $aRb \Rightarrow (c \square a)\ R\ (c \square b)$; R is *compatible with* $\square \Leftrightarrow a, b \in S$, $\forall\, c, d \in S$, $(aRb,\ cRd) \Rightarrow (a \square c)\ R\ (b \square d)$.

Right compatibility is defined in a similar manner Further equality is compatible with all laws of composition

Theorem 10 1 If R is a transitive and reflexive relation defined in a set S having a law of internal composition $\Box$ then R is compatible with $\Box \Leftrightarrow R$ is both left and right compatible with $\Box$

Problem 10 1 Define right compatibility

Problem 10 2 Prove Theorem 10 1

Problem 10 3 Determine if R of Example 10 2 is compatible with $\bigcirc$ of illustrative Example 4 1

Problem 10 4 Let $H = \{a\ b\ c\}$ Find three relations defined in H each in turn having one but only one of the properties of Definition 10 2

11 INEQUALITY IN N

Definition 11 1 $a\ b \in N\ a > b \Leftrightarrow \exists c \in N \ni a = b + c$ $a < b \Leftrightarrow b > a$ $a \geqslant b \Leftrightarrow (a > b \text{ or } a = b)$ $a \leqslant b \Leftrightarrow b \geqslant a$

Theorem 11 1 $a\ b \in N \Rightarrow$ *exactly one* of the following holds

(1) $a = b$
(2) $a > b$
(3) $a < b$

Proof This is Theorem 8 2 restated in terms of inequality

Theorem 11 2 $a > b$ is a transitive relation in N

Proof We must show $a\ b\ c \in N \Rightarrow (a > b \quad b > c \Rightarrow a > c)$ Now $a > b \Rightarrow \exists d \in N \ni a = b + d$ $b > c \Rightarrow \exists e \in N \ni b = c + e$ Therefore $a = (c + e) + d = c + (e + d)$ by associativity and so $a > c$ since $e + d \in N$ by Theorem 7 1 ■

Theorem 11 3 $a > b$ is compatible with addition and with multiplication in N

In the next eight problems all letters represent natural numbers If in a problem one or more natural numbers must be excluded to have the general statement hold the reader is expected to state such exclusions

Problem 11 1 Prove $a + c > b + c \Rightarrow a > b$

PROBLEM 11.2. Prove: $a > b \Rightarrow a \geqslant b + 1$.

PROBLEM 11.3. Prove: $a < b \Rightarrow a + 1 \leqslant b$.

PROBLEM 11.4. Prove: $\forall\, a \in N, a \geqslant 1$.

PROBLEM 11.5. Prove: $a \in N \Rightarrow \nexists\, b \in N \ni a < b < a + 1$.

PROBLEM 11.6. Prove: $a < b + 1 \Rightarrow a \leqslant b$.

PROBLEM 11.7. Prove: $ac > bc \Rightarrow a > b$.

PROBLEM 11.8. Prove: $a, b \in N, a > b \Rightarrow \nexists\, c \in N \ni a + c = b$.

PROBLEM 11.9. Prove Theorem 11.3.

PROBLEM 11.10. Prove Theorem 11.4 below.

THEOREM 11.4. The cancellation law holds for multiplication and all elements of N.

Our final theorem of this chapter is equivalent to the statement that every nonempty set of natural numbers has a smallest number in it.

THEOREM 11.5. Let L be a nonempty set of natural numbers. Then $\exists\, s_0 \in L \ni \forall\, s \in L, s \geqslant s_0$.

PROOF: Suppose that the theorem is false. Then for each $t \in L\ \exists\, s_t \in L \ni s_t < t$. Let $M = \{x | x \in N$ and $x \notin L$ and $x \leqslant s$, $\forall\, s \in L\}$. Then $1 \in M$, since $1 \leqslant n$ by Problem 11.4, $\forall\, n \in N$ and if $1 \in L$, there would be, by the condition at the beginning of the proof (implied by the supposition of falsity), a natural number $s_1 < 1$.

Let $x \in M$. Then by Problem 11.3, $x^+ = x + 1 \leqslant s$, $\forall\, s \in L$. If $x + 1 \in L$, then $\exists\, y \in L \ni y < x + 1$, i.e., $y \leqslant x$ by Problem 11.6. But since $x \in M$, $x < y$ since $y \in L$. Therefore, $x^+ \notin L$ so $x^+ \in M$. Therefore, $x \in M \Rightarrow x^+ \in M$. Therefore, $M = N$ and L must be empty, contrary to hypothesis. Hence, our supposition is false and the theorem is true. ■

PROBLEM 11.11. Prove that if a set of natural numbers L satisfies: (1) $n \in L$, (2) $(x \in L, x > n) \Rightarrow x^+ \in L$, then L contains the set of all natural numbers $\geqslant n$.

PROBLEM 11.12. Prove that if a set of natural numbers L satisfies: (1) $1 \in L$, (2) $(a \in L, \forall\, a < x) \Rightarrow x \in L$, then $L = N$.

Chapter 2 Semigroups, Equivalence Relations, and Rational Integers

In this chapter we consider semigroups and begin our study of groups. To do this conveniently, we consider some further properties of mappings, since certain properties of many systems, such as the associative laws, can be proved most easily by relating them to a set of mappings.

Then we introduce a generalization of the idea of equality, an equivalence relation, which is of extreme importance in a great many of our subsequent developments. We also introduce the concept of isomorphism, which tells us when two mathematical systems are abstractly identical. We consider the formation of new systems from old ones by taking set products and quotient sets with respect to equivalence relations; also considered are the means by which laws of composition in the old systems induce laws of composition in the new ones.

Finally we apply the ideas developed thus far to derive the system of the rational integers, and we consider congruence modulo m in that system.

1 SEMIGROUPS

In Chapter 1 we considered various general properties of sets and developed the important properties of the particular mathematical system of the natural numbers. We shall not at present define a general mathematical system, but we now consider a very elementary mathematical system of a general kind.

Definition 1.1 A *semigroup* is a nonempty set S and an associative law of internal composition defined everywhere in S.

We shall, for most of this chapter, denote this law by $\square$ and denote the semigroup by $(S, \square)$. Occasionally, if the law of composition is clear from the context, we may denote the semigroup by S.

If $\square$ is commutative, then we shall say that the semigroup $\langle S; \square\rangle$ is commutative.

It should be emphasized that a semigroup is a set *and* a law of composition. Often we encounter sets with two or more laws of composition and it may be that the set and each of these laws form different semigroups. For example, $\langle N; +\rangle$ is a semigroup; also $\langle N; \cdot\rangle$ is a semigroup and the two semigroups are different. For brevity, we often shall refer to these semigroups as the additive and multiplicative semigroups of N, respectively.

PROBLEM 1.1. Let P be the set of all subsets of a nonempty set S.

(a) Prove that P and $\cup$ form a semigroup.
(b) Prove that P and $\cap$ form a semigroup.

PROBLEM 1.2. Find three subsets of N which together with one of the laws of composition defined in N form semigroups.

2. PRODUCTS OF MAPPINGS

In order to have some easy and informative examples of semigroups and their properties, we shall now consider a law of composition for mappings and investigate the important properties of this law. Henceforth, many of these results will be of the utmost importance.

In order to illustrate the definitions and theorems given, we shall give first a particular set of mappings. We let $H = \{a, b, c\}$ and we let $\mathscr{S}_3$ be the set of all mappings of H into itself. For any set with a small number of elements, such as H, one convenient way of giving such a mapping is to write two rows: in the upper put all the elements of H, and in the lower below each element of H (in the upper row) write its image. Thus, some of the mappings of $\mathscr{S}_3$ are:

$$\iota = \begin{pmatrix} abc \\ abc \end{pmatrix}, \quad \alpha = \begin{pmatrix} abc \\ bca \end{pmatrix}, \quad \beta = \begin{pmatrix} abc \\ cab \end{pmatrix}, \quad \gamma = \begin{pmatrix} abc \\ acb \end{pmatrix}, \quad \delta = \begin{pmatrix} abc \\ cba \end{pmatrix},$$

$$\epsilon = \begin{pmatrix} abc \\ bac \end{pmatrix}, \quad \zeta = \begin{pmatrix} abc \\ aaa \end{pmatrix}, \quad \eta = \begin{pmatrix} abc \\ aab \end{pmatrix}, \quad \theta = \begin{pmatrix} abc \\ aba \end{pmatrix}, \quad \kappa = \begin{pmatrix} abc \\ caa \end{pmatrix},$$

$$\lambda = \begin{pmatrix} abc \\ ccc \end{pmatrix}, \quad \mu = \begin{pmatrix} abc \\ baa \end{pmatrix}, \quad \sigma = \begin{pmatrix} abc \\ bbb \end{pmatrix}, \quad \tau = \begin{pmatrix} abc \\ ccc \end{pmatrix}.$$

The reader may easily complete the list. There are 27 such mappings as a moment's reflection will disclose.

The above method of exhibiting a mapping is not practical for a set having infinitely many elements, such as N. However, if the set has one or more laws of composition defined in it, such as N does, a very useful way of giving a mapping is by means of a formula. Thus one mapping, call it α, of N into itself is given by $x\alpha = ax + b$, where $a, b \in N$; this gives the image $x\alpha$ of each element of N.

DEFINITION 2.1. Let α be a mapping of a set S into a set T and β be a mapping of T into a set U. Then the *product* $\alpha\beta$ is the mapping of S into U defined by $x(\alpha\beta) = (x\alpha)\beta$, $\forall x \in S$.

EXAMPLE 2.1. For the particular α, γ defined above (mappings of H into itself), we have $a(\alpha\gamma) = (a\alpha)\gamma = b\gamma = c$, $b(\alpha\gamma) = (b\alpha)\gamma = c\gamma = b$, $c(\alpha\gamma) = (c\alpha)\gamma = a\gamma = a$. Thus, by Definition 3.2 of Chapter 1, $\alpha\gamma = \delta$. Or more compactly, this product is $\alpha\gamma = \begin{pmatrix} abc \\ bca \end{pmatrix}\begin{pmatrix} abc \\ acb \end{pmatrix} = \begin{pmatrix} abc \\ bca \end{pmatrix}\begin{pmatrix} bca \\ cba \end{pmatrix} = \begin{pmatrix} abc \\ cba \end{pmatrix} = \delta$, since clearly $\begin{pmatrix} abc \\ acb \end{pmatrix}$ and $\begin{pmatrix} bca \\ cba \end{pmatrix}$ are the same mapping.

PROBLEM 2.1. Find $\alpha\eta$ and $\eta\kappa$.

PROBLEM 2.2. Show that $\zeta\eta$ and $\zeta\gamma$ are both equal to ζ.

PROBLEM 2.3. Find $\iota\eta$; show that the product of ι and any mapping $\xi \in \mathscr{S}_3$, in either order, is the mapping ξ.

PROBLEM 2.4. Find $\alpha\beta$ and $\beta\alpha$, where α and β are the two mappings of N itself defined by $x\alpha = x + 2$ and $x\beta = 3x + 4$.

THEOREM 2.1. Let α be a mapping of S into T, β a mapping of T into U, γ a mapping of U into V. Then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.

PROOF. Let $x \in S$. We apply Definition 2.1 repeatedly and find that $(\alpha\beta)\gamma$ is the mapping $\ni x[(\alpha\beta)\gamma] = [x(\alpha\beta)]\gamma = [(x\alpha)\beta]\gamma$, $\forall x \in S$; $\alpha(\beta\gamma)$ is the mapping $\ni x[\alpha(\beta\gamma)] = (x\alpha)(\beta\gamma) = [(x\alpha)\beta]\gamma$, $\forall x \in S$. Therefore, by Definition 3.2 of Chapter 1, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$. ∎

PROBLEM 2.5. For the mappings of $\mathscr{S}_3$, find (a) $\alpha(\epsilon\delta)$ and $(\alpha\epsilon)\delta$, (b) $\beta(\eta\theta)$ and $(\beta\eta)\theta$.

PROBLEM 2.6. For α, β as in Problem 2.4 and γ defined by $x\gamma = 5x + 2$, find $\alpha(\beta\gamma)$ and $(\alpha\beta)\gamma$.

THEOREM 2.2. The set of all mappings of a nonempty set E into itself and the product as defined in Definition 2.1 form a semigroup.

PROBLEM 2.7. Prove Theorem 2.2.

3. THE ASSOCIATIVE LAW GENERALIZED

Thus far we have considered composites of not more than three elements of the system under consideration. For a composite of three elements, $a \square b \square c$, we have the associative law which tells us that whether we combine a and b first, or b and c, the ultimate result is the same. If we have more than three elements, the situation becomes more complicated. For example, with four elements, a, b, c, d, we can combine them in different manners as follows: $[(a \square b) \square c] \square d$, $(a \square b) \square (c \square d)$, $a \square [b \square (c \square d)]$. The more elements there are to be combined, the more different ways there are to combine them. However, it is a remarkable fact that all the different ways give the same result as long as the associative law holds for merely any three elements. To prove this last statement would require an extremely detailed analysis of the combinatorial possibilities, which is beyond the scope of this book and not needed in the book. We shall merely prove a theorem (Theorem 3.1) which covers a very important case and which is illustrative of the theorem needed in the general case. To carry out the proof we shall define the composite of n elements in one particular way and then show that certain other groupings give the same result. First, however, we make a definition which will also be useful later

DEFINITION 3.1. Let $n \in N$. Then a *finite sequence* of elements of a set E is $\{a_i\}_{i=1,2,\ldots,n}$ as defined in Definition 4.2 of Chapter 1, with order defined as: $a_i < a_j \Leftrightarrow i < j$; or, the set $\{a_{c_i}\}_{i=1,2,\ldots,n}$ where $c_i \in N$ and $a_{c_i} < a_{c_j} \Leftrightarrow i < j$.

Now we are ready to define a particular composite of a finite sequence of elements and do it by specifying that each new element comes on the left and is combined with the composite of the others already combined. We could do it equally well on the right. The definition is of course by induction.

DEFINITION 3.2. Let $\{a_i\}_{i=1,2,\ldots,n}$ be a finite sequence of elements from the semigroup $\langle S; \square \rangle$, $n \in N$. Then $\square_{i=k}^{k} a_i = a_k$, $\forall k \leqslant n$, and $\square_{i=1}^{n} a_i = a_1 \square (\square_{i=2}^{n} a_i)$, for $n \geqslant 1$.

If $\{a_{c_j}\}_{j=1,2,\ldots,m}$ is a finite sequence of elements of the semigroup $\langle S; \square \rangle$, then $\square_{j=1}^{m} a_{c_j} = \square_{j=1}^{m} b_j$, where $b_j = a_{c_j}$.

This last part covers the case of composites in which the first factor on the left does not have the subscript 1, and other cases.

In case $\square = +$, then $\square_{i=1}^{n} a_i$ is usually written $\Sigma_{i=1}^{n} a_i$. In case $\square = \cdot$, then $\square_{i=1}^{n} a_i$ is usually written $\Pi_{i=1}^{n} a_i$.

The collecting of factors in this composite means that for four elements we take the grouping as $a_1 \square [a_2 \square (a_3 \square a_4)]$

If we have a composite $(a_1 \square a_2) \square (a_3 \square a_4 \square a_5) \square a_6 \square (a_7 \square a_8)$ this could be written as a composite of four elements $b_1 \square b_2 \square b_3 \square b_4$ where $b_1 = a_1 \square a_2$ $b_2 = a_3 \square a_4 \square a_5$ $b_3 = a_6$ $b_4 = a_7 \square a_8$ This illustrates the notation of the next theorem

THEOREM 3 1 Let $b_1 = \square_{i=1}^{i_1} a_i$ $b_2 = \square_{i=i_1+1}^{i_2} a_i$ $b_k = \square_{i=i_{k-1}+1}^{n} a_i$ be any grouping of the elements in the composite $\square_{i=1}^{n} a_i$ where the $a_i \in (S \ \square)$ which is a semigroup Then $\square_{i=1}^{n} a_i = \square_{j=1}^{k} b_j$

PROOF We proceed by induction on n The theorem is obviously true if $n = 1$ and we shall suppose it true for any number of a less than n (cf Problem 11 12 of Chapter 1) We distinguish two cases

(1) $i_1 = 1$ Then $b_1 = a_1$ Then $\square_{j=1}^{k} b_j = b_1 \square (\square_{j=2}^{k} b_j) = a_1 \square (\square_{j=2}^{k} b_j)$ By induction hypothesis $\square_{j=2}^{k} b_j = \square_{i=2}^{n} a_i$ Therefore, by Definition 3 2 $\square_{j=1}^{k} b_j = \square_{i=1}^{n} a_i$

(2) $i_1 > 1$ Then let $b_1' = \square_{i=2}^{i_1} a_i$ Then by induction hypothesis $b_1' \square (\square_{j=2}^{k} b_j) = (\square_{i=2}^{n} a_i)$ Now by the associative law and Definition 3 2 $a_1 \square (b_1' \square (\square_{j=2}^{k} b_j)) = (a_1 \square b_1') \square (\square_{j=2}^{k} b_j) = b_1 \square (\square_{j=2}^{k} b_j) = \square_{j=1}^{k} b_j$ But by the induction hypothesis and Definition 3 2 $a_1 \square (b_1' \square (\square_{j=2}^{k} b_j)) = a_1 \square (\square_{i=2}^{n} a_i) = \square_{i=1}^{n} a_i$ Therefore $\square_{i=1}^{n} a_i = \square_{j=1}^{k} b_j$ ■

PROBLEM 3 1 In the semigroup $\mathscr{S}_3$ find the product $\alpha\gamma\eta\beta$ in three different ways How do we know that $\mathscr{S}_3$ is a semigroup?

PROBLEM 3 2 Using α β of Problem 2 4 γ of Problem 2 6 and δ defined by $x\delta = 4x + 1$ $\forall x \in N$ find $\alpha\beta\gamma\delta$ in two different ways

DEFINITION 3 3 In Definition 3 2 if $a_1 = a_2 = \cdots = a_n = a$ we write $\square_{i=1}^{n} a_i = a^n$ unless the law of composition $\square$ is addition in which case we write (usually) $\square_{i=1}^{n} a_i = na$ In either case n is called an *exponent* multiplicative or additive as the case may be a^n is called a *power* of a

In Problems 3 3 3 4 and 3 5 a $b \in (S \ \square)$ a semigroup and $a \square b = b \square a$ (Use induction in the proofs)

PROBLEM 3 3 Prove $a^n \square a^m = a^{n+m}$

PROBLEM 3 4 Prove $(a^n)^m = a^{nm}$

PROBLEM 3 5 Prove $(a \square b)^n = a^n \square b^n$

PROBLEM 3 6 For $\mathscr{S}_3$ find α^3 ι^2 γ^4 ζ^7 η^4 θ

PROBLEM 3.7. Find α^3 for α of Problem 2.4.

PROBLEM 3.8. Prove: $a \in \langle S; \square \rangle$, a semigroup, $x = a^k, y = a^j$, $k, j \in N \Rightarrow x \square y = y \square x$.

PROBLEM 3.9. For $E \in P$, for P of Problem 1.1, find E^n for $\square = \cup$ and $\square = \cap$.

4. SUBSEMIGROUPS

Frequently we shall have occasion to consider a subset of the set of elements in a semigroup, and it will be of interest to know if this subset and the original law of composition form a semigroup. To make this consideration formally precise we introduce the following definitions.

DEFINITION 4.1. Let $\square$ be a law of internal composition between elements of a set S (cf. Definition 4.2 of Chapter 1) defined on a subset A of $S \times S$; we shall call the law *induced by* $\square$ on a subset T of S, that law of composition between elements of T defined on the set of (x, y) of $T \times T \ni (x, y) \in A$ and $x \square y \in T$, and which is such that it makes the composite $x \square y$ correspond to (x, y).

DEFINITION 4.2. Let $\langle S; \square \rangle$ be a semigroup, $T \subset S$, and $\square_1$ the law of composition induced in T by $\square$. Then T and $\square_1$ form a *subsemigroup of* $\langle S; \square \rangle \Leftrightarrow \langle T; \square_1 \rangle$ is a semigroup.

It is vital to remember that to have a subset of a semigroup be a subsemigroup, the law of composition must be the same (i.e., it must be induced in the subset) as that of the larger set. For example, in N the set consisting of 1 and "$\cdot$" form a subsemigroup of $\langle N; \cdot \rangle$, but, of course, not of $\langle N; + \rangle$.

Sometimes, for brevity, we may say that T is a subsemigroup of the semigroup S, and by that we shall mean that the law of composition in T is understood to be as above.

In Pioblems 4.1 through 4.5 show that the given set of elements is a subsemigroup of $\mathscr{S}_3$. If an English letter is given, that letter is used in the future to refer to this subsemigroup.

PROBLEM 4.1. H: ζ, σ, τ.

PROBLEM 4.2. S_3: $\iota, \alpha, \beta, \gamma, \delta, \epsilon$.

PROBLEM 4.3. ι.

PROBLEM 4.4 $\iota. \alpha, \beta$.

PROBLEM 4.5. All powers of any particular element of $\mathscr{S}_3$.

PROBLEM 4.6 Find three more subsemigroups of $\mathscr{S}_3$.

5 NEUTRAL ELEMENTS AND INVERSE ELEMENTS

In N the element 1 has the property that $a \cdot 1 = 1 \cdot a = a$ $\forall a \in N$. Since nothing happens to another element when 1 is combined with it by multiplication, it is reasonable to consider the element 1 as neutral with respect to multiplication. In $\mathscr{S}_3$, ι has the same property. We generalize this property in the next definition.

DEFINITION 5.1 Let $(S, \square)$ be a semigroup. Then $e_L \in S$ ($e_R \in S$) is a *left (right) neutral element* of $S \Leftrightarrow \forall a \in S$, $e_L \square a = a$ ($a \square e_R = a$). $e \in S$ is a *neutral element of* $S \Leftrightarrow e$ is both a right and a left neutral element of S.

THEOREM 5.1 If a semigroup has a neutral element, the neutral element is unique.

PROBLEM 5.1 Prove Theorem 5.1. (Hint: let e, f both be neutral elements and show that $e = f$.)

PROBLEM 5.2 Give four examples of semigroups which have neutral elements.

PROBLEM 5.3 Give four examples of semigroups which do *not* have neutral elements.

PROBLEM 5.4 Show that ζ, σ, τ of H of Problem 4.1 are all left neutral elements of H, but that none is a right neutral element—hence, that none is a neutral element.

In Problem 4.4, $\alpha\beta = \iota$ and ι is the neutral element of the semigroup in this problem. So in a sense β undoes α and might therefore be considered inverse to α. In Problem 4.2, $\gamma\gamma = \iota$ and so γ is its own inverse. We generalize this.

DEFINITION 5.2 Let $(S, \square)$ be a semigroup with a neutral element e. Then $a \in S$ has a *left (right) inverse* $\Leftrightarrow \exists b \in S$ ($c \in S$) $\ni b \square a = e$ ($a \square c = e$). The element b (c) is called the *left (right) inverse of* a. The element $a \in S$ has an *inverse* $\Leftrightarrow$ it has a left inverse and a right inverse which are equal.

The inverse of a is usually denoted by a^{-1}, unless the law of composition is addition and then it is denoted by $-a$.

THEOREM 5.2 $a \in (S, \square)$, a semigroup with a neutral element, has a left inverse b and a right inverse $c \Rightarrow b = c$.

THEOREM 5.3. $a \in \langle S; \Box\rangle$, a semigroup with a neutral element, has an inverse $\Rightarrow$ the inverse is unique.

PROBLEM 5.5. Prove Theorem 5.2.

PROBLEM 5.6. Prove Theorem 5.3.

PROBLEM 5.7. Find the neutral elements (if any) and the elements which have inverses (if any) in $\langle N; +\rangle$ and in $\langle N; \cdot\rangle$.

PROBLEM 5.8. Show that every element of S_3 of Problem 4.2 has an inverse.

PROBLEM 5.9. Show that the only elements of $\mathscr{S}_3$ which have inverses are the elements of S_3 (cf. Problem 5.8).

THEOREM 5.4. $a, b \in \langle S; \Box\rangle$, a semigroup with a neutral element, a^{-1}, b^{-1} exist $\Rightarrow (a \Box b)^{-1}$ exists and $(a \Box b)^{-1} = b^{-1} \Box a^{-1}$.

THEOREM 5.5. In a semigroup with a neutral element, the left (right) cancellation law holds for each element which has a left (right) inverse.

PROBLEM 5.10. Prove Theorem 5.4. (Hint: show that $b^{-1} \Box a^{-1}$ is an inverse and apply Theorem 5.3.)

PROBLEM 5.11. Generalize Theorem 5.4 to more than two factors.

PROBLEM 5.12. Prove Theorem 5.5.

PROBLEM 5.13. Using Theorem 5.5 and Problem 2.2, show that ζ of $\mathscr{S}_3$ does not have an inverse.

PROBLEM 5.14. Find three other elements of $\mathscr{S}_3$ which do not have inverses.

6. DEFINITION OF A GROUP

The mathematical system naturally suggested by the introduction of the concepts of neutral element and inverse is a group. We shall give three equivalent definitions of this very important system (and a fourth in a problem).

DEFINITION 6.1a. A semigroup $\langle G; \Box\rangle$, with a neutral element and an inverse for each element, is a *group*. The *order* of the group $\langle G; \Box\rangle$ is the number of elements of G. A group (or semigroup) is called *finite* $\Leftrightarrow$ it has only a finite number of elements.

DEFINITION 6 1b A *group* is a set of elements G and a law of internal composition $\Box$ which satisfy

(1) $\forall a\ b \in G\ \exists c \in G \ni a \Box b = c$

(2) $\forall a\ b\ c \in G\ \ a \Box (b \Box c) = (a \Box b) \Box c,$

(3) $\exists e \in G \ni \forall a \in G\ \ a \Box e = e \Box a = a$

(4) $\forall a \in G\ \exists a^{-1} \in G \ni a^{-1} \Box a = a \Box a^{-1} = e$

DEFINITION 6 1c A *group* is a nonempty set of elements G and a law of internal composition $\Box$ which satisfy

(1) $\forall a\ b \in G\ \exists c \in G \ni a \Box b = c$

(2) $\forall a\ b\ c \in G\ \ a \Box (b \Box c) = (a \Box b) \Box c$

(3) $\forall a\ b \in G\ \exists x\ y \in G \ni a \Box x = b\ \ y \Box a = b$

DEFINITION 6 2 A *subgroup* of a group G is a subsemigroup of G which is a group

THEOREM 6 1 A finite semigroup in which the cancellation law holds for each element is a group

PROBLEM 6 1 Prove that Definitions 6 1a 6 1b and 6 1c are equivalent (Hint the most difficult part of this is showing that Definition 6 1c ⇒ Definition 6 1b To do this first show that for a particular element a there exists a neutral element for a Then show that this neutral element for a is a neutral element of the group)

PROBLEM 6 2 Prove Theorem 6 1 (Hint let $a_1\ a_2 \quad a_n$ be the distinct elements of the semigroup Form the composites of all these by one of them and show that Definition 6 1c holds)

PROBLEM 6 3 Prove that a semigroup S which satisfies the following two conditions is a group (1) $\exists e \ni e \Box a = a\ \ \forall a \in S$ (2) $\forall a \in S\ \exists a_l \ni a_l \Box a = e_l$

PROBLEM 6 4 Determine which of the semigroups so far considered are groups

PROBLEM 6 5 Prove that the cancellation law holds for every element in a group

PROBLEM 6 6 Let S be a semigroup with a neutral element Prove that the set of all elements of S which have inverses in S form a subsemigroup of S and that this semigroup is a group

PROBLEM 6 7 Prove that S_3 of Problem 4 2 is a group

7 A THEOREM ABOUT MAPPINGS

THEOREM 7 1 The set of all 1–1 mappings of a nonempty set

E onto itself and the law of composition of Definition 2.1 form a group.

PROOF: We shall show that the conditions of Definition 6.1b are satisfied.

Condition 1. Let α, β be any two 1–1 mappings of E onto itself.

First, we shall show that $\alpha\beta$ is a mapping of E onto itself (it is of course a mapping of E into itself). Since α, β are mappings of E onto itself, given any $x'' \in E$, $\exists\, x' \in E \ni x'' = x'\beta$ and $\exists\, x \in E \ni x' = x\alpha$. Then $x'' = x'\beta = (x\alpha)\beta = x(\alpha\beta)$. So x'' is the image of x under $\alpha\beta$. Therefore, $\alpha\beta$ is a mapping of E *onto* itself.

Secondly, we shall show that $\alpha\beta$ is a 1–1 mapping. Given $x'' \in E$, from the above we know that $\exists\, x \in E \ni x'' = x(\alpha\beta)$. Suppose that for some $y \in E$, $x'' = y(\alpha\beta)$. Let $y' = y\alpha$; then $x'' = y'\beta$. Since β is a 1–1 mapping, $y' = x'$, so $x' = y\alpha$. Since α is a 1–1 mapping, $x = y$. Therefore, $\alpha\beta$ is a 1–1 mapping.

Condition 2. This follows from Theorem 2.2.

Condition 3. We define ι by $\forall\, x \in E$, $x\iota = x$. Then ι is obviously a 1–1 mapping of E onto itself. Now $\forall\, x \in E$, $x(\iota\alpha) = (x\iota)\alpha = x\alpha \Rightarrow \iota\alpha = \alpha$. Also $x(\alpha\iota) = (x\alpha)\iota = x\alpha$, since $x\alpha \in E$. Therefore, $\alpha\iota = \iota = \iota\alpha$. Therefore, ι is a neutral element.

Condition 4. Let α be any 1–1 mapping of E onto itself. Let β be defined as follows: given $x \in E$, $x\beta$ is the element $x' \in E$ determined by $x = x'\alpha$. (This x' exists since α is an onto mapping, and there is only one such x' since α is a 1–1 mapping.) Then $x\beta$ is defined $\forall\, x \in E$ and so β is a mapping of E into itself.

Suppose $\exists\, x, y \in E \ni x' = x\beta, x' = y\beta$. Then $x = x'\alpha$ and $y = x'\alpha$ and so $x = y$. Therefore, β is a 1–1 mapping.

Next, given $x' \in E$, we wish to show that $\exists\, x \in E \ni x' = x\beta$. Now $x' = x\beta \Leftrightarrow x = x'\alpha$. Since α is a mapping of E into itself, given $x' \in E$, $\exists\, x \in E \ni x = x'\alpha$ and so $x' = x\beta$. Therefore, β is an onto mapping.

Lastly, this mapping β which we have established as a 1–1 mapping of E onto itself, is the inverse of α. For by proceeding as above for any $x \in E$, $x' = x\beta$, we have $x(\beta\alpha) = (x\beta)\alpha = x'\alpha = x = x\iota$. Also, for any $x' \in E$, $x = x'\alpha$, and so $x'(\alpha\beta) = (x'\alpha)\beta = x\beta = x' = x'\iota$. Therefore, $\beta\alpha = \alpha\beta = \iota$. Hence, β is the inverse of α.

Therefore, the set and the law of composition form a group. ■

8. EQUIVALENCE RELATIONS

Certain properties of relations were discussed in Section 10 of Chapter 1. We now introduce a name for relations which possess some of these properties

DEFINITION 8 1 A relation R defined in a set S is an *equivalence relation* $\Leftrightarrow R$ is reflexive symmetric and transitive

Thus for many purposes an equivalence relation acts like equality which of course is a particular equivalence relation Any equivalence relation determines a separation of the set S into a collection of subsets of a kind which we now define

DEFINITION 8 2 A *partition* Π of a set S is a collection of nonempty subsets such that
(1) S is the union of all the sets of Π
(2) every two distinct sets of Π are disjoint

THEOREM 8 1 An equivalence relation R defined in a nonempty set S determines a partition of S

PROOF $\forall a \in S$ let $C_a = \{x | x \in S \text{ and } xRa\}$ C_a is nonempty since by reflexivity $a \in C_a$ Also since $a \in C_a$ S is the union of the C Finally let $C_a \cap C_b \neq \varnothing$ let $d \in C \cap C_b$ Then dRa dRb Now let $x \in C_b$ Then xRb $bRd \Rightarrow xRa$ by the symmetric and transitive properties of R Thus $x \in C_a$ and so $C_b \subset C_a$ Similarly $C_a \subset C_b$ Therefore $C_a = C_b$ Thus we have established that either $C_a \cap C_b = \varnothing$ or $C_a = C_b$ Therefore the distinct C_a $a \in S$ are disjoint Therefore the collection of all the distinct C_a is a partition of S ■

The sets C_a are worthy of a name

DEFINITION 8 3 (a) The sets of a partition of a set S determined by an equivalence relation R defined in S are *equivalence classes* determined by R sometimes called equivalence classes modulo R

(b) The set of these equivalence classes is called the *quotient set of S by R* and is written S/R

An equivalence relation and a partition are essentially the same Theorem 8 1 goes halfway in establishing this and the next theorem completes the process

THEOREM 8 2 A partition Π of a nonempty set S determines an equivalence relation R in S when R is defined by ($aRb \Leftrightarrow a$ $b \in$ the same subset in Π)

PROBLEM 8 1 Prove Theorem 8 2

PROBLEM 8.2. For the set H of Example 4.3 of Chapter 1, consider the partition $H = \{a\} \cup \{b, c\}$. Determine whether or not the equivalence relation determined by this partition is compatible with the law of composition given in the example.

Soon we are going to develop·the system of the rational integers. To do this we shall find it convenient to use certain general methods which are useful in many developments. Among these methods are two by means of which we frequently obtain new algebraic systems from previously known ones. One of the methods uses the set product of Definition 4.1 of Chapter 1, and the other uses quotient sets and equivalence relations. We now consider the first method.

9. SEMIGROUP PRODUCTS OF SEMIGROUPS

DEFINITION 9.1. Let $\langle S; \square\rangle$ and $\langle T; \bigcirc\rangle$ be two semigroups (groups). Then the *semigroup (group) product* of $\langle S; \square\rangle$ and $\langle T; \bigcirc\rangle$, written $S \times T$, is the set of all ordered pairs (s, t) where $s \in S$ and $t \in T$, with a law of internal composition $\triangle$ defined by $(s_1, t_1) \triangle (s_2, t_2) = (s_1 \square s_2, t_1 \bigcirc t_2)$.

THEOREM 9.1. The semigroup (group) product of two semigroups (groups) is a semigroup (group).

EXAMPLE 9.1. Let $K_1 = \{\iota, \alpha, \beta\}$ and $K_2 = \{\iota, \gamma\}$, considered as subgroups of $\mathcal{S}_3$. Then the group product of these two groups consists of the elements (ι, ι), (ι, γ), (α, ι), (α, γ), (β, ι), (β, γ) with the composites of a few of these elements as follows: $(\iota, \gamma)(\beta, \gamma) = (\beta, \iota)$; $(\alpha, \gamma)(\beta, \iota) = (\iota, \gamma)$, etc. The group product is of course a group.

EXAMPLE 9.2. We can consider $N \times N$ as a semigroup product in more than one way since there are two laws of composition defined in N. With addition, we have $(a, b) + (c, d) = (a + c, b + d)$ and with multiplication, $(a, b) \cdot (c, d) = (ac, bd)$. We shall presently consider rather extensively $N \times N$ with addition so defined but with a different law of multiplication.

PROBLEM 9.1. Prove Theorem 9.1.

PROBLEM 9.2. Let $K_3 = \{\iota, \delta\}$, $K_4 = \{\iota, \epsilon\}$, as in $\mathcal{S}_3$. Find $K_2 \times K_3$, $K_2 \times K_4$, $K_3 \times K_4$, where K_2 is given in Example 9.1 above.

PROBLEM 9.3. Find $K_1 \times K_1$, where K_1 is given in Example 9.1 above.

Problem 9.4. Find $K_2 \times K_2$ with K_2 of Example 9.1.

Problem 9.5. Prove that if K, L are subsemigroups (subgroups) of two semigroups (groups) S, T respectively, then $K \times L$ is a subsemigroup (subgroup) of $S \times T$.

10. COMPOSITION TABLE OF A SEMIGROUP

By *the composition table of a semigroup* we mean a rectangular array with each column labelled with one element of the semigroup, each row labelled with one element of the semigroup, and the entry in the intersection of the row labelled x with the column labelled y being the composite $x \square y$. The composition table of the subgroup K_3 of $\mathscr{S}_3$ is given here.

	ι	α	β
ι	ι	α	β
α	α	β	ι
β	β	ι	α

Problem 10.1. Construct the composition table for $K_2 \times K_3$ and $K_2 \times K_4$ of Problem 9.2.

Problem 10.2. Construct the composition table for the semigroup consisting of the following mappings of $\{a, b, c, d\}$ into itself: $\omega, \omega^2, \omega^3, \iota$, where $\omega = \begin{pmatrix} abcd \\ bcda \end{pmatrix}$, $\iota = \begin{pmatrix} abcd \\ abcd \end{pmatrix}$. Show that it is a group.

Problem 10.3. Construct the composition table for $K_1 \times K_2$ of Example 9.1.

Problem 10.4. Construct the composition table for S_3 of Problem 4.2.

It should be observed that in the composition table of a group each element of the group appears exactly once in each row and exactly once in each column. This follows from Problem 6.5. This may not be the case in a semigroup. Also, in the composition table of a group or a semigroup, if the elements are given in the same order in the labelling row as in the labelling column, then the law of composition of the group or semigroup is commutative if and only if the table is symmetric with respect to the diagonal running from upper left to lower right.

11. HOMOMORPHISMS AND ISOMORPHISMS

In abstiact algebra we concern ourselves mainly with those properties of algebraic systems which depend on how the elements of a system combine with each other and we are usually not concerned with other, more concrete, properties of the elements. Thus we introduce a term, isomorphic, to denote two systems such that we can establish a 1–1 correspondence between the elements so that corresponding elements combine similarly. Isomorphic systems, for many purposes, are considered identical. We now define this and make a generalization.

DEFINITION 11.1. Let $\langle S; \square\rangle$ and $\langle T; \bigcirc\rangle$ be two semigroups. Then a mapping α of S into T is a *homomorphism of S into T* $\Leftrightarrow \forall\, s_1, s_2 \in S$, $(s_1 \square s_2)\,\alpha = (s_1\alpha) \bigcirc (s_2\alpha)$.

The mapping α is a homomorphism of $\langle S; \square\rangle$ *onto* $\langle T; \bigcirc\rangle \Leftrightarrow \alpha$ is a homomorphism of S into T, and α is an onto mapping. Here, we say that T is *homomorphic to S*. (We use this for brevity; when the laws of composition are understood. For completeness we should say $\langle T; \bigcirc\rangle$ is homomorphic to $\langle S; \square\rangle$.)

The homomorphism α is an *isomorphism of S onto T*, or *an isomorphism between S and T* $\Leftrightarrow \alpha$ is a 1–1 mapping of S onto T. Then and only then we say that S and T are *isomorphic*.

A homomorphism of S into itself is called an *endomorphism*.

An isomorphism of S onto itself is called an *automorphism*.

EXAMPLE 11.1. Consider $K_2 = \{\iota, \gamma\}$, $K_3 = \{\iota, \delta\}$, as subgroups of S_3. If we define the mapping A by $\iota A = \iota$, $\gamma A = \delta$, then A is an isomoiphism between K_2 and K_3. It is obviously a 1–1 mapping of K_2 onto K_3. To establish the composition preserving property, we must consider all possible composites of two elements of K_2 and show that each such composite is mapped onto the composite of the images undei A. There are four such composites: $\iota\cdot\iota$, $\iota\cdot\gamma$, $\gamma\cdot\iota$, $\gamma\cdot\gamma$. They are equal to, respectively, ι, γ, γ, ι, and are mapped onto ι, δ, δ, ι. On the other hand, $(\iota A)(\iota A) = \iota\cdot\iota = \iota$, $(\iota A)(\gamma A) = \iota\cdot\delta = \delta$, $(\gamma A)(\iota A) = \delta\cdot\iota = \delta$, $(\gamma A)(\gamma A) = \delta\cdot\delta = \iota$. Therefore, A is an isomorphism and K_2 is isomorphic to K_3.

The method used in this example can become rather tedious. Another method, often more convenient in the case of systems with only a few elements, is to use the composition tables of the two systems. If we have two semigroups, each with n elements, which we wish to show are isomorphic, then let us arrange the composition tables as follows: in the ith position of the labelling row of the second semigroup table place the element which is the image under a supposed isomorphism of the element in the ith place of the labelling row of the first semigroup table for $i = 1$ 2 n operate in a similar manner on the columns Then the supposed isomorphism will actually be an isomorphism if and only if each entry in the body of the second table is the image of the element in the same position in the first table In the case of groups with large numbers of elements usually the most practical way of establishing an isomorphism is by the use of formulae

PROBLEM 11 1 Show that $K_2 \times K_3$ $K_2 \times K_4$ $K_3 \times K_4$ of Problem 1 1 are isomorphic

PROBLEM 11 2 Show that the group of Problem 10 2 is not isomorphic to any of the groups of Problem 11 1

PROBLEM 11 3 Show that S_3 of Problem 4 2 is not isomorphic to $K_1 \times K_2$ of Problem 10 3

PROBLEM 11 4 Prove if S is a semigroup homomorphic (isomorphic) to T and T is homomorphic (isomorphic) to U then S is homomorphic (isomorphic) to U Use this to prove that the relation of being homomorphic or isomorphic is an equivalence relation in the set of all semigroups

PROBLEM 11 5 Show that S_3 of Problem 4 2 is homomorphic to K_2 and K_3 Note that the mappings giving these homomorphisms of S_3 into K_2 and K_3 are endomorphisms of S_3 since K_2 and K_3 are subgroups of S_3 Show that S_3 is *not* homomorphic to K_1

PROBLEM 11 6 Show that for K $\iota \leftrightarrow \iota$ $\alpha \leftrightarrow \beta$ $\beta \leftrightarrow \alpha$ is an automorphism (Note the symbol $\leftrightarrow$ is used only for 1 1 mappings)

Notice that in Problems 11 7 through 11 11 α is a homomorphism of a semigroup S into a semigroup T

PROBLEM 11 7 Prove that $S\alpha$ (cf Definition 3 1 of Chapter I) and the law of composition of T form a subsemigroup of T

PROBLEM 11 8 Prove that if S has a neutral element e then $e\alpha$ is a neutral element for $S\alpha$

PROBLEM 11 9 Prove that if S has a neutral element and if $a \in S$ has an inverse (or a left or right inverse) then that inverse must be mapped onto an element of T which is an inverse for $a\alpha$

PROBLEM 11 10 If S is a group prove that $S\alpha$ is a subgroup of T

PROBLEM 11.11. If T has a neutral element, prove that the set of all elements of S which are mapped onto that neutral element is a subsemigroup (subgroup if S is a group) of S.

Having the concept of isomorphism available we can now define precisely what we mean by extending an algebraic system in the case of semigroups.

DEFINITION 11.2. The semigroup S is *imbedded* in the semigroup $U \Leftrightarrow \exists\, a$ subsemigroup T of $U \ni S$ and T are isomorphic. The semigroup U is called an *extension* of S.

PROBLEM 11.12. Prove that if S and T are two semigroups with neutral elements, then S and T are both imbedded in $S \times T$.

12. INDUCING LAWS OF COMPOSITION IN QUOTIENT SETS

We are now going to consider the second method of extending algebraic systems as discussed at the end of Section 8, namely by means of taking quotient sets. The most vital condition is compatibility of the equivalence relation used in forming the quotient set, with the law or laws of composition in the original set.

THEOREM 12.1. Let E be a set closed with respect to a law of internal composition $\Box$, and let R be an equivalence relation defined in E and compatible (cf. Definition 10.3 of Chapter 1) with $\Box$. Then a law of internal composition $\overline{\Box}$ can be defined in E/R such that

(1) E/R is closed under $\overline{\Box}$,

(2) for $A, B, C \in E/R, A \mathbin{\overline{\Box}} B = C \Leftrightarrow \forall\, a \in A, \forall\, b \in B, \exists\, c \in C \ni a \Box b = c$.

This law $\overline{\Box}$ is said to be *induced* in E/R by $\Box$ of E.

PROOF: To find $A \mathbin{\overline{\Box}} B$, for any $A, B \in E/R$, let $x \in A, y \in B$. Since E is closed under $\Box$, $\exists\, z \in E \ni x \Box y = z$. Since E is the union of the sets comprising E/R, $\exists\, C \in E/R \ni z \in C$. Then we define $A \mathbin{\overline{\Box}} B = C$. Now we wish to show that C is independent of the particular x and y chosen from A and B, respectively. Let a, b be any elements of A, B, respectively. Then xRa and yRb. Now R is, by hypothesis, compatible with $\Box$, and so $xRa, yRb \Rightarrow (x \Box y)R(a \Box b)$ $\Rightarrow zR(a \Box b) \Rightarrow a \Box b \in C$. Thus, C is independent of the choice of the representatives of A and B, and so we have the final statement in the theorem.

■

THEOREM 12 2 **Under the conditions** of Theorem 12 1, if $\square$ is associative, then $\overline{\square}$ is associative

THEOREM 12 3 **Under the conditions** of Theorem 12 1, if $\square$ is commutative, then $\overline{\square}$ is **commutative**

THEOREM 12 4 **Under the conditions** of Theorem 12 1, if E is closed under Δ, **a second law of internal composition** if R is compatible with Δ and if Δ is **left (right) distributive** with respect to $\square$ then if $\overline{\Delta}$ denotes the **law induced in** E/R **by** Δ we have $\overline{\Delta}$ as left (right) distributive with respect to $\overline{\square}$

PROBLEM 12 1 **Prove Theorem** 12 2

PROBLEM 12 2 **Prove Theorem** 12 3

PROBLEM 12 3 **Prove Theorem** 12 4

PROBLEM 12 4 **Prove that under the conditions of Theorem** 12 1 if E has a **neutral element then** E/R has a **neutral element Consider inverses**

We are going to consider $N \times N$ to obtain the system of the rational integers but the next result may just as well be stated under more general conditions so we do so The reader might for ease in following the proof think of S as N and of $\square$ as $+$

THEOREM 12 5 **Let** $(S\ \square)$ **be a commutative** semigroup in which the cancellation law holds for each element and let $L = S \times S$ be the semigroup product of S with itself Then $(a\ b)R(c\ d) \Leftrightarrow a \square d = b \square c$ is an equivalence relation defined in L and compatible with $\overline{\square}$, the law of composition induced in $S \times S$ by $\square$ (Cf Definition 9 1)

PROOF First, we prove that R is an equivalence relation in L

(1) R is reflexive since $a \square b = b \square a$, since S is commutative

(2) R is symmetric since $a \square d = b \square c \Rightarrow c \square b = d \square a$, since S is commutative

(3) R is transitive $(a\ b)R(c\ d)\ (c\ d)R(e\ f) \Rightarrow a \square d = b \square c$, and $c \square f = d \square e$ Multiplying the first of these equations by f on the right and the second by b on the left we have $a \square d \square f = b \square c \square f$, $b \square c \square f = b \square d \square e$ whence we have $a \square d \square f = b \square d \square e \Rightarrow a \square f = b \square e$, by **commutativity** and cancellation law Therefore, $(a, b)R(e\ f)$

Now to show **compatibility** $(a, b)R(c\ d) \Leftrightarrow a \square d = b \square c$ $(e,f)R(g,h) \Leftrightarrow e \square h = f \square g$ Now $(a\ b)\ \overline{\square}\ (e,f) = (a \square e\ b \square f)$, $(c, d)\ \overline{\square}\ (g, h) = (c \square g, d \square h)$ To demonstrate compatibility we must show that $(a, b)\,\overline{\Box}\,(e, f)R(c, d)\,\overline{\Box}\,(g, h)$. But this follows immediately from the last four equations above by commutativity and associativity. ■

Definition 12.1. For N considered as an additive (a multiplicative) semigroup, R of the above theorem for $N \times N$ will be denoted by R_1 (by R_2).

Problem 12.5. For R_1 (R_2) as above, find several elements in the equivalence class containing $(1, 5)$. Show that $(7, 4)\not{R}_i(3, 6)$ for $i = 1, 2$.

Problem 12.6. Carry out the proof of Theorem 12.5 for $N \times N$ and addition; for $N \times N$ and multiplication.

We now state a theorem about $N \times N$, using a different multiplication, not the one induced by that in N.

Theorem 12.6. In $P = N \times N$, with N as an additive semigroup, we define $(a, b) \cdot (c, d) = (ac + bd,\ ad + bc)$. Then P is closed with respect to this law of composition and R_1 is compatible with it.

Problem 12.7. Prove Theorem 12.6.

Problem 12.8. Prove: in $P' = N \times N$, with N as a multiplicative semigroup, define $(a, b) + (c, d) = (ad + bc, bd)$; then P' is closed with respect to this law of composition and R_2 is compatible with it.

Problem 12.9. Prove the following generalization of Theorem 12.5.

Theorem 12.7. Let $\langle S; \Box\rangle$ be a commutative semigroup, S^* be the set of elements of S for which the cancellation law holds, $S^* \neq \varnothing$, $M = S \times S^*$, the semigroup product. Then $(a, b)R(c, d) \Leftrightarrow a \Box d = b \Box c$ is an equivalence relation defined in M and compatible with $\overline{\Box}$, the law induced in $S \times S^*$ by $\Box$, as in Definition 9.1.

In this chapter we shall apply the next theorem only to N, and so S^* will also be N. Thus the reader may think of this in reading the proof. We shall state and prove it in more general form.

Theorem 12.8. Let $\langle S: \Box\rangle$ be a commutative semigroup, S^* the set of elements of S for which the cancellation law holds, S^* nonempty. Then there exists a commutative semigroup T such that

(1) S is imbedded in T,

(2) T has a neutral element.

(3) $x \in S^* \Rightarrow \exists x^{-1} \in T$.

(4) T is the smallest semigroup having properties (1), (2), and (3).

PROOF. To avoid needlessly complicated notation we shall use $\square$ to indicate the law induced in $N \times N$ by $\square$, and $\{(u, v)\}$ to denote the equivalence class containing (u, v).

Let $T = (S \times S^*)/R$, where R is the equivalence relation of Theorem 12.7.

(1) Let W be the set of all equivalence classes containing all elements $(u \square v, v)$ where $u \in S$, $v \in S^*$. We shall prove that $u \to \{(u \square v, v) | \forall v \in S^*\}$ is an isomorphism.

First, we note that all $(u \square v, v)$ belong to the same equivalence class since $u \square v \square v_1 = v \square u \square v_1 \Rightarrow (u \square v, v) R (u \square v_1, v_1)$ and the equations hold since S is associative and commutative. Now let $u_1 \to \{(u_1 \square v_1, v_1)\}$ and $u_2 \to \{(u_2 \square v_2, v_2)\}$ and suppose $(u_1 \square v_1, v_1) R (u_2 \square v_2, v_2)$. Then $u_1 \square v_1 \square v_2 = v_1 \square u_2 \square v_2 \Rightarrow u_1 = u_2$ since $v_1, v_2 \in S^*$. Therefore the mapping is 1-1 and it is onto by definition.

That $u_1 \square u_2 \to \{(u_1 \square v_1, v_1)\} \overline{\square} \{(u_2 \square v_2, v_2)\}$ where $\overline{\square}$ is the law induced in T by $\square$ is obvious. Therefore we have an isomorphism between W and S, and since T is a semigroup, S is imbedded in T.

(2) The equivalence class containing (u, u) for any $u \in S^*$ is the neutral element of T. For $(u, v) \square (u, u) = (u \square u, v \square u) R (u, v)$. Therefore $\{(u, v)\} \overline{\square} \{(u, u)\} = \{(u, v)\}$.

(3) For $u \in S^*$, $(u \square v, v) \square (v, u \square v) = (u \square v \square v, v \square u \square v) R (u, u) R (v, v)$. Therefore $\{(u \square v, v)\} \overline{\square} \{(v, u \square v)\} = \{(u, u)\}$. Therefore if $u \in S^*$, its image in T under the isomorphism of part (1) of the proof has an inverse. Hence, by identifying u with that image, u has an inverse in T.

(4) Let V be the set of all equivalence classes which are inverses of elements of T corresponding to elements of S^*. We shall show that condition (4) of the conclusion of the theorem holds by showing that every elment of T is the composite of an element of W and an element of V. From this, (4) will follow since any semigroup having the first three properties must contain all these composites.

Let (a, b) be any element of $S \times S^*$ and let $v, u \in S^*$. Then $(a, b) R (a \square v, v) \square (u, u \square b) = (a \square v \square u, v \square u \square b)$ since $a \square v \square u \square b = b \square a \square v \square u$ since S is associative and commutative. Therefore each equivalence class of T is the composite of an equivalence class of W, since $(a \square v, v)$ is a representative of such a class, and an equivalence class of V, since $(u, v \square b)$ is a representative of such a class because $u, b \in S^*$. ∎

COROLLARY 12.1. If the cancellation law holds for every element of S, then the semigroup T, of Theorem 12.8 is a group.

COROLLARY 12.2. The additive semigroup of N can be imbedded in a group.

PROBLEM 12.10. Go over the proof of Theorem 12.8 with N as S, addition as $\square$, and R_1 as R; also with N as S, multiplication as $\square$, and R_2 as R.

THEOREM 12.9. The multiplication in $N \times N$, as defined in Theorem 12.6, is associative, commutative, and distributive with respect to the addition induced in $N \times N$ by addition in N. Further, the multiplication induced in $(N \times N)/R_1$ by this multiplication in $N \times N$ is associative, commutative, and distributive with respect to the addition in $(N \times N)/R_1$ induced by the addition in $N \times N$.

PROBLEM 12.11. Prove Theorem 12.9. (Hint: use Theorems 12.1 through 12.4, and other results.)

13. DEFINITION OF THE RATIONAL INTEGERS

DEFINITION 13.1. (Thc Rational Integers.) The additive group, $Z = (N \times N)/R_1$, whose existence is established by Theorem 12.8 (with $\square = +$) and Corollary 12.1, with multiplication defined in Theorem 12.6, is called the *ring of rational integers*. An element of Z is called a *rational integer*, sometimes, when the context is clear, merely an *integer*. The additive neutral element of Z will be denoted by 0, and the additive inverse of $a \in Z$ by $-a$. Finally, for brevity we shall usually write $a - b$ for $a + (-b)$.

THEOREM 13.1. The elements of Z and addition form a commutative group; the elements of Z and multiplication form a commutative semigroup with a neutral element, usually denoted by 1; the cancellation laws hold for addition for every element, and for multiplication foı every nonzero element; multiplication is distributive with respect to addition; the additive semigroup of N and the multiplicative semigroup of N are imbedded in the additive and multiplicative (respectively) semigroups of Z.

PROBLEM 13.1. Prove Theorem 13.1. (Most of the theorem has been proved. The cancellation laws and the imbedding statement have not. For the latter, use the mapping $a \leftrightarrow \{(a+1, 1)\}, \forall a \in N$.)

Since by Theorem 13.1, N is imbedded in Z, we can refer to N as being contained in Z for all properties involving addition and multiplication. As for the "less than" relation, we now generalize it to Z and in doing so leave unchanged all that we had for N in this connection.

Definition 13.2. For any $x \in Z$, x is an equivalence class determined by an ordered pair $(a, b) \in N \times N$. We shall say that x is *positive* $\Leftrightarrow a > b$ and say that x is *negative* $\Leftrightarrow a < b$. If x is positive, we write $x > 0$; if negative, $x < 0$. For any $x, y \in Z$, we write $x > y \Leftrightarrow x - y > 0$; $x \geq y \Leftrightarrow (x > y \text{ or } x = y)$. Lastly, we shall use Z^* to denote the set of all $x \in Z \ni x > 0$.

Theorem 13.2. Every rational integer is exactly one of the following: positive, negative or zero.

Theorem 13.3. The elements of N are those rational integers which are positive.

Theorem 13.4. The relation $<$ is transitive and is compatible with addition in Z. (However, we do not have complete compatibility with multiplication.)

Theorem 13.5. $a, b, c, d \in Z$, $a > b$, $c > 0$, $d < 0 \Rightarrow ac > bc$, $ad < bd$.

Problem 13.2. Prove Theorems 13.2, 13.3, 13.4 and 13.5.

Problem 13.3. Consider the statements in Problems 11.1 through 11.8 of Chapter 1 with regard to whether they hold in Z. Make any alterations necessary to have them hold in Z if that is possible. Then prove the altered statements.

Problem 13.4. Restate and prove for Z Theorem 11.5 and Problems 11.11 and 11.12 of Chapter 1.

Problem 13.5. Prove: $a \in Z$, $a < 0 \Rightarrow \exists b \in Z^* \ni a = (-1)b$, $a + b = 0$.

14. ABSOLUTE VALUE OF RATIONAL INTEGERS

Definition 14.1. Let $a \in Z$. Then $|a| = a$ if $a \geq 0$; $|a| = -a$ if $a < 0$.

Theorem 14.1. $a, b \in Z \Rightarrow |a + b| \leq |a| + |b|$, $|ab| = |a||b|$.

Problem 14.1. Prove Theorem 14.1. (Hint: one way is to consider four cases.)

15. EXPONENTS

Previously we defined (Definition 3.3) exponents and powers with natural numbers as exponents. We now generalize this to rational integers as exponents and do it in a general semigroup with a neutral element e.

Definition 15.1. Let $\langle S; \square \rangle$ be a semigroup with a neutral element e. Then $\square_{\iota \in \varnothing}\ a_\iota = e, a_\iota \in S$; multiplicatively, $a^0 = e$, where $0 \in Z$. If $n \in Z^{>}$, a^n is defined as in Definition 3.3. If $a \in S$ has an inverse a^{-1}, then for $m \in Z^{>}$, $a^{-m} = (a^{-1})^m$ (cf. Problem 13.5).

Theorem 15.1. Let $a, b \in \langle S; \square \rangle$, a semigroup with neutral element. Let $a^{-1}, b^{-1} \in S$ and $a \square b = b \square a$. Then $\forall\, n, m \in Z$,
(1) $a^n \square a^m = a^{n+m}$,
(2) $(a^n)^m = a^{nm}$,
(3) $(a \square b)^n = a^n \square b^n$.

Problem 15.1. Prove Theorem 15.1. (Hint: use Problems 3.3, 3.4, 3.5.)

Problem 15.2. Write out the statements of Definition 15.1 and Theorem 15.1 for $\square = +$.

16. DIVISIBILITY IN A SEMIGROUP

In this chapter we are principally interested in Z, but it is essentially as easy to give definitions about divisibility in a rather general semigroup as it is in Z, so we shall do so.

In the following eight definitions, S is a semigroup with a neutral element and the law of composition is written as multiplication.

Definition 16.1. $a \in S$, a is a *left (right) multiple* of $b \in S$ $\Leftrightarrow \exists\, c \in S \ni a = cb$ $(a = bc)$. Under these conditions, b is a *right (left) divisor of* a. If multiplication is commutative in S, we simply say, multiple and divisor, and write, $b|a$.

Problem 16.1. Find three examples of multiples and divisors in the semigroups studied thus far.

Definition 16.2. $a \in S$, a is a *unit* in $S \Leftrightarrow a$ has an inverse in S.

Problem 16.2. Prove that the only units in Z are ± 1.

Definition 16 3 a $b \in S$ are *associates* in $S \Leftrightarrow \exists$ a unit $u \in S \ni a = bu$ or $a = ub$

Problem 16 3 Prove $a \in Z \Rightarrow$ the only associates of a in Z are a and $-a$

Problem 16 4 Prove that the relation of being associates is an equivalence relation

Definition 16 4 Let $b \in S$ and let b be a divisor of a Then b is a *proper divisor* of $a \Leftrightarrow$

(1) b is not an associate of a

(2) b is not a unit

Definition 16 5 $a \in S$ is *irreducible in S* $\Leftrightarrow$

(1) a is not a unit in S

(2) a has no proper divisors in S

Definition 16 6 Let S be commutative and let the cancellation law hold for every element of S Then if p is not a unit $p \in S$ is a *prime* in S $\Leftrightarrow$ ($p|ab$ a $b \in S \Rightarrow$ either $p|a$ or $p|b$) An element of Z is a prime if and only if it is a prime in the multiplicative semigroup of Z with zero excluded

The reader may have encountered a definition of prime which is the above definition of irreducible element We shall show that in Z the property of being irreducible is equivalent to the property of being prime In some algebraic systems the two properties are not equivalent

Definition 16 7 $d \in S$ d is a *greatest common left (right) divisor* of a $b \in S \Leftrightarrow$

(1) d is a left (right) divisor of a and of b

(2) $f \in S$ f is a left (right) divisor of a and of $b \Rightarrow d$ is a right (left) multiple of f

If S is commutative right and left greatest common divisors coincide (We abbreviate left greatest common divisor by l g c d etc)

It should be noted that this definition is in terms of divisibility alone The reader may have encountered definitions of greatest common divisor and least common multiple of two integers in which the conditions were given in terms of magnitude Such definitions do not generalize easily to other algebraic systems Definition 16 7 does

Definition 16 8 $m \in S$ m is a *least common left (right) multiple* of a $b \in S \Leftrightarrow$

(1) m is a left (right) multiple of a and of b

(2) $k \in S$, k is a left (right) multiple of a and of $b \Rightarrow m$ is a right (left) divisor of k.

If S is commutative, right and left least common multiples coincide. (We abbreviate by l.l.c.m., etc.)

Problem 16.5. Prove: $a, b, c \in S$, $c|a$, $c|b \Rightarrow c|(a+b)$, $c|(a-b)$.

Problem 16.6. Prove: $a, b, c \in S$, a semigroup, $(c|a$ or $c|b) \Rightarrow c|ab$.

Problem 16.7. Prove that in a semigroup, the relation $a|b$ is reflexive and transitive.

17. DIVISIBILITY IN Z

In the next exercises, some of the particular properties of Z are necessary.

Problem 17.1. Prove: $a, b \in Z$, a is a proper divisor of $b \neq 0 \Rightarrow |a| < |b|$; thus, $a, b \in Z$, $a \neq 0 \Rightarrow |ab| \geqslant |b|$.

Problem 17.2. Prove: $r_1, r_2, a \in Z, 0 \leqslant r_1 < a, 0 \leqslant r_2 < a \Rightarrow |r_1 - r_2| < a$.

Problem 17.3. If M is a set of nonnegative rational integers with the properties $0 \in M$ and $x \in M \Rightarrow x + 1 \in M$, then M is the set of all nonnegative rational integers.

We next state and prove the division algorithm for Z. The proof given needs to be modified only slightly to hold in some more general algebraic systems.

Theorem 17.1. $a, b \in Z$, $a \geqslant 0$, $b > 0 \Rightarrow \exists$ unique $q, r \in Z \ni a = bq + r$, $q \geqslant 0$, $0 \leqslant r < b$.

Proof: We use Problem 17.3. Let $b \in Z$, $b > 0$ and let $M = \{a | a \in Z, a \geqslant 0, \exists\, q, r \in Z \ni a = bq + r, q \geqslant 0, 0 \leqslant r < b\}$.

For $a = 0$, $a = bq + r$, where $q = r = 0$ and so $0 \in M$.

Let $a \in M$. Then $\exists\, q, r \in Z \ni a = bq + r$, $q \geqslant 0$, $0 \leqslant r < b$. Then $a + 1 = bq + r + 1$. Since $r < b$, by Problem 11.3 of Chapter 1 generalized in Problem 13.3 of this chapter, $r + 1 \leqslant b$. If $r + 1 < b$, we have $a + 1 \in M$ with $r + 1$ as the new r. If $r + 1 = b$, then $a + 1 = b(q + 1)$ and so $a + 1 \in M$ with $q + 1$ as the new q, and 0 as the new r. Therefore, M contains all nonnegative rational integers.

To prove uniqueness, let $a = bq_1 + r_1$, $0 \leqslant r_1 < b$, $q_1 \geqslant 0$. Then

$bq_1 + r_1 = bq + r$, $b(q - q_1) = r_1 - r$ and by Problem 17.2 $|r - r_1| < b$ and so by Problem 17.1 $q - q_1 = 0 \Rightarrow q = q_1$, $r = r_1$. ∎

Problem 17.4. Generalize the above theorem by permitting a to be any rational integer and b to be any rational nonzero integer, changing the conclusion slightly so that the generalization will be correct. Prove the generalization. (Hint: induction is not necessary.)

Theorem 17.2. $a, b \in Z$, both a, b not zero, have a greatest common divisor (least common multiple) $\Rightarrow a, b$ have a positive greatest common divisor denoted by (a, b) (positive least common multiple denoted by $[a, b]$).

Problem 17.5. Prove Theorem 17.2. (Note that this theorem does *not* state that two integers have a g.c.d. or an l.c.m.)

Problem 17.6. Consider the situation in Theorem 17.2 if a or b or both are zero.

Theorem 17.3. $a, b \in Z$, $a \geq 0$, $b \geq 0$, a and b not both zero $\Rightarrow \exists\, s, t \in Z \ni sa + tb = (a, b)$.

Proof. Consider $I = \{z \mid z \in Z,\ z = ax + by$ where $x, y \in Z\}$. For $x = 1$, $y = 0$ and for $x = 0$, $y = 1$ we see that $a \in I$, $b \in I$. Therefore I contains at least one positive rational integer and by Theorem 11.5 of Chapter 1 and Theorem 13.3 of this chapter it contains a smallest positive rational integer $d = x_1a + y_1b$. Then by Theorem 17.1 $\exists\, q, r \in Z \ni a = qd + r$, $0 \leq r < d$. Then $r = 1 \cdot a + (-q) \cdot d = 1 \cdot a + (-q)(x_1a + y_1b) = (1 - qx_1)a + (-qy_1)b$. Therefore $r \in I$. But since $0 \leq r < d$ and d is the smallest positive integer in I, $r = 0$. Therefore $a = qd$. Therefore $d|a$ and similarly $d|b$. Therefore d is a common divisor of a and b. Let d_1 be any common divisor of a and b; then $a = kd_1$, $b = md_1$ where $k, m \in Z$. Then from $d = x_1a + y_1b = x_1kd_1 + y_1md_1 = (x_1k + y_1m)d_1$ we see that $d_1|d$. Therefore since $d > 0$, by Definition 16.7 and Theorem 17.2, $d = (a, b)$. Take $s = x_1$, $t = y_1$ and we have the theorem. ∎

Problem 17.7. Prove $a, b \in Z$, $a^2 + b^2 \neq 0 \Rightarrow \exists\, s, t \in Z \ni sa + tb = (a, b)$.

Problem 17.8. Find s and t of Theorem 17.3 for $a = 326$ and $b = 424$.

Definition 17.1. $a, b \in Z$ are *relatively prime* $\Leftrightarrow (a, b) = 1$. Also, a is called *prime to b* and b *prime to a* $\Leftrightarrow (a, b) = 1$.

Theorem 17.4. $a, b, c \in Z$, $a|bc$, $(a, b) = 1 \Rightarrow a|c$.

PROBLEM 17.9. Prove Theorem 17.4. (Hint: use the result of Problem 17.7.)

THEOREM 17.5. $p, b_1, b_2, \ldots, b_k \in Z, p|b_1b_2 \cdots b_k, p$ a prime $\Rightarrow \exists\, i \ni p|b_i, 1 \leqslant i \leqslant k$.

PROOF: Let M be the set of positive rational integers, k, for which the theorem holds. Obviously, $1 \in M$, since if $k = 1, i = 1$. Let $k \in M$ and let $p|b_1b_2 \cdots b_kb_{k+1}$. Now either $p|b_{k+1}$, in which case $i = k+1$, or $(p, b_{k+1}) = 1 \Rightarrow p|b_1b_2 \cdots b_k$ by Theorem 17.4. Then since $k \in M$, $\exists\, i \ni p|b_i$, $1 \leqslant i \leqslant k$. Therefore, $k + 1 \in M$. Therefore, the theorem is true for any finite number of factors. ■

LEMMA. $a, p \in Z$, p irreducible $\Rightarrow (a, p) = 1$ or $(a, p) = |p|$.

PROOF: Let p be positive. If $(a, p) = k$, where $1 < k < p$, then $k|p$, which is impossible (by Definition 16.5). The case of negative p is left to the reader. ■

THEOREM 17.6. $p \in Z$, p is irreducible $\Leftrightarrow p$ is prime.

PROOF: First consider the implication $\Rightarrow$. Let p be irreducible and let $p|ab$, i.e., $ab = kp$, where $k \in Z$. By the above lemma, either $(a, p) = |p| \Rightarrow p|a$, or $(a, p) = 1 \Rightarrow p|b$, by Theorem 17.4.

Now consider the implication $\Leftarrow$. Let p be a prime. Suppose $p = ab$, where neither a nor b is a unit. Then by Problem 17.1, $|p| > |a|$, $|p| > |b|$. But, since $p = ab$ can be written $p \cdot 1 = ab$, we have $p|ab$ and since p is a prime, either $p|a$ or $p|b$, which contradicts Problem 17.1. ■

18. UNIQUE FACTORIZATION

We shall now give a general definition which for the present we shall apply to Z only.

DEFINITION 18.1. Let $a \in S$, a commutative semigroup with a neutral element and multiplication as the law of composition. Further, let a be expressible as $a = p_1p_2 \cdots p_r$, where the $p_1, p_2, \cdots, p_r$ are irreducible in S. This *factorization is essentially unique* $\Leftrightarrow$ whenever $a = p_1'p_2' \cdots p_t'$, where the $p_1', p_2', \ldots, p_r'$ are irreducible in S, then $r = t$ and $\exists$ a 1–1 mapping ϕ of $\{1, 2, \ldots, n\}$ onto itself $\ni$ each p_i is an associate of $p_{\phi(i)}'$. This last condition is a rigorous way of saying that there is an arrangement of the p_j' so that each p_i is an associate of p_i'.

Sometimes, for brevity, the adjective "essentially" is omitted.

THEOREM 18 1 **(Essentially unique factorization theorem for Z)** Let $a \in Z$, a not a unit and $a \neq 0$ Then a has an essentially unique factorization as a product of primes [Since, in Z, primes are irreducible elements (and conversely) we say primes here instead of irreducible elements]

PROOF First, we prove the existence of such a factorization and then prove it unique Since if $a < 0$, then $a = u(-a)$, where u is a unit, we may suppose that a is positive We shall use Problem 11 12 of Chapter 1 as generalized by Problem 13 4 of this chapter

Let $M = \{a | a \in Z, a > 0, (a = 1, \text{ or } a \text{ has a factorization as a product of primes})\}$ Then $1 \in M$

Let $x \in M$ $\forall x < a$ Then either a is a prime, and so $a \in M$ or $a = cd$ where c $d \in Z$ and neither c nor d is a unit nor an associate of a Then by Problem 17 1 $1 < c < a, 1 < d < a \Rightarrow c, d \in M$ So a is equal to the product of the factorizations of c and d Therefore, $a \in M$ and so the existence of a factorization is established

Now let K be the set of positive integers k such that for integers having k prime factors in a factorization as a product of primes, that factorization is essentially unique

Now $1 \in K$ by Theorem 17 6 Let $k \in K$ and let $a \in Z$ have the two factorizations $a = p_1p_2 \quad p_kp_{k+1}$ and $a = q_1q_2 \quad q_{j+1}$ where the p_i and q_r are prime and $j \geqslant k$ Now since p_{k+1} is a prime by Theorem 17 5 $p_{k+1} | q_s$ for some s $1 \leqslant s \leqslant j + 1$ Without loss of generality we may assume by renumbering the q s if necessary, that $p_{k+1} | q_{j+1}$ Then by applying the cancellation law, we have $p_1p_2 \quad p_k = q_1q_2 \quad q_ju$, where u is a unit But now on the left side of this last equation, we have an element of Z which has a factorization into a product of k primes, so since $k \in K$ this factorization is essentially unique and so each $p_i |$ some q_r Therefore $k \in K \Rightarrow k + 1 \in K$ Therefore, factorization is essentially unique for any finite number of factors ■

COROLLARY 18 1 $a \in Z$ $a \neq 0$ 1 -1, a has the distinct prime factors $p_1, p_2, \quad , p_n \Rightarrow a = ep_1^{\alpha_1}p_2^{\alpha_2} \quad p_n^{\alpha_n}$, $\alpha_i \in N$, $e = \pm 1$, and the α_i are unique

PROBLEM 18 1 **Prove the above corollary**

PROBLEM 18 2 **Prove** $a, b \in Z$ $(a \ b) = d, a = a_1d, b = b_1d \Rightarrow (a_1, b_1) = 1$

PROBLEM 18 3 **Prove** a $b \in Z \Rightarrow [a \ b](a, b) = |ab|$

19 CONGRUENCES

We now define an extremely **important** equivalence relation in Z

DEFINITION 19.1. Let $a, b, m \in Z$. Then $a \equiv b \mod m \Leftrightarrow m | (a - b)$. This relation is read "a is congruent to b modulo m." The integer m is called the *modulus*.

THEOREM 19.1. Congruence modulo m is an equivalence relation compatible with addition and multiplication in Z.

PROBLEM 19.1. Prove Theorem 19.1.

DEFINITION 19.2. The equivalence classes determined by congruence modulo m are called *residue classes modulo m*. The quotient set of Z with respect to congruence modulo m is denoted by Z_m, with addition and multiplication induced by that in Z (cf. Theorem 12.1).

THEOREM 19.2. $a, m \in Z, m \neq 0 \Rightarrow \exists\, r \in Z \ni a \equiv r \mod m$ and $0 \leqslant r < |m|$.

COROLLARY 19.1. Z_m has $|m|$ elements.

PROBLEM 19.2. Prove Theorem 19.2.

PROBLEM 19.3. Prove Corollary 19.1.

DEFINITION 19.3. $r_1, r_2, \ldots, r_m \in Z$ is a *complete set of residues modulo m* $\Leftrightarrow r_i \not\equiv r_j \mod m$ for $i \neq j$. The set, $0, 1, \ldots, m - 1$ is called the complete set of *least residues modulo m*. A set, $r_1, r_2, \ldots, r_s$, obtained from a complete set of residues by deleting those numbers which have a factor in common with m, is called a *reduced set of residues modulo m*.

THEOREM 19.3. The number of elements in one reduced set of residues modulo m is the same as in every other reduced set of residues modulo m.

THEOREM 19.4. A set of integers $r_1, r_2, \ldots, r_s$ is a reduced set of residues modulo $m \Leftrightarrow$

(1) $r_i \not\equiv r_j$ for $i \neq j, i, j = 1, 2, \ldots, s$
(2) $(m, r_i) = 1, i = 1, 2, \ldots, s$
(3) $a \in Z, (a, m) = 1 \Rightarrow \exists\, i \ni a \equiv r_i, 1 \leqslant i \leqslant s$.

PROBLEM 19.4. Prove Theorem 19.3.

PROBLEM 19.5. Prove Theorem 19.4.

DEFINITION 19.4. The number of integers in a reduced set of residues modulo m is denoted by $\phi(m)$ and is called the *totient function* and also *Euler's ϕ-function*.

In Z_m, the cancellation law of addition holds for every element, but, for multiplication, the best result is that which is given in the second conclusion of the following theorem.

THEOREM 19.5. $a, b, c \in Z \Rightarrow (a + c \equiv b + c \mod m \Rightarrow a \equiv b \mod m)$ and $(a \cdot c \equiv b \cdot c \mod m \Rightarrow a \equiv b \mod m_1$, where $m_1 = m/(c, m))$.

PROOF. The first conclusion is obvious. For the proof of the second, let $d = (c, m)$. Now $ac \equiv bc \mod m \Rightarrow \exists k \in Z \ni ac = bc + km$ where $k \in Z$. Let $c = c_1 d$. By hypothesis, $m = dm_1$, where $m_1 \in Z$. Then we have $ac_1 = bc_1 d + km_1 d \Rightarrow ac_1 = bc_1 + km_1 \Rightarrow (a - b)c_1 = km_1 \Rightarrow c_1 | k \Rightarrow a - b = k_1 m_1$, where $k_1 = k/c_1 \Rightarrow a \equiv b \mod m_1$. ∎

COROLLARY 19.2. $ac \equiv bc \mod m, (c, m) = 1 \Rightarrow a \equiv b \mod m$.

PROBLEM 19.6. Give an example showing that the last statement of Theorem 19.5 cannot be improved.

LEMMA. $a, b, c \in Z, (a, b) = 1, a > 0, b > 0 \Rightarrow r, a + r, 2a + r, \ldots, (b - 1)a + r$ *form a complete set of residues modulo* b.

PROOF. Since there are b integers in the set, we need merely show that no two are congruent modulo b. Suppose $na + r \equiv ma + r \mod b$ with $0 \leq n \leq b$, $0 \leq m \leq b$. Then by Theorem 19.5 $ma \equiv na \mod b$ and by Corollary 19.2 $n \equiv m \mod b$ and so $n = m$ by the inequalities satisfied by n and m. ∎

THEOREM 19.6. $a, b \in Z, (a, b) = 1 \Rightarrow \phi(a)\phi(b) = \phi(ab)$.

PROOF. The expression $aq + r$ for $r = 0, 1, \ldots, a - 1$ and $q = 0, 1, \ldots, b - 1$ gives without repetition all nonnegative integers less than ab. Clearly, $aq + r$ is prime to $a \Leftrightarrow (a, r) = 1$. Let r_1 be one of those $\phi(a)$ integers (i.e., which are prime to a). Then by the above lemma, there are among $r_1, a + r_1, 2a + r_1, \ldots, (b - 1)a + r_1$ exactly $\phi(b)$ integers prime to b. Therefore there are exactly $\phi(a)\phi(b)$ nonnegative integers less than ab and prime to both a and b. Therefore $\phi(a)\phi(b) = \phi(ab)$. ∎

THEOREM 19.7. $p \in Z, p$ a prime, $n \in N \Rightarrow \phi(p^n) = p^{n-1}(p - 1) = p^n(1 - 1/p)$.

THEOREM 19.8. $m \in Z, p_1, p_2, \ldots, p_k$ are the distinct prime factors of $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} > 0 \Rightarrow \phi(m) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1) = m(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$.

PROBLEM 19.7. Prove Theorem 19.7.

PROBLEM 19.8. Prove Theorem 19.8.

Problem 19.9. Prove: q is the product of the distinct prime factors common to m_1 and $m_2 \Rightarrow \phi(m_1m_2) = q(\phi(m_1)\phi(m_2)/\phi(q))$.

Theorem 19.9. (Fermat–Euler) $a, m \in Z$, $(a, m) = 1$, $m > 0$ $\Rightarrow a^{\phi(m)} \equiv 1 \bmod m$.

Proof: Let $a_1, a_2, \ldots, a_{\phi(m)}$ be a reduced set of residues modulo m. Then the set of integers $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is also a reduced set. For, if $aa_i \equiv aa_j \bmod m$, then by Corollary 19.2, $a_i \equiv a_j \bmod m$, which contradicts the hypotheses made about the a_i. Therefore, $a_i \equiv aa_{n_i} \bmod m$, for $i = 1, 2, \ldots, \phi(m)$ and suitably chosen n_i, by Theorem 19.4. Now by multiplying these congruences together, we get $a_1a_2 \cdots a_{\phi(m)} \equiv a^{\phi(m)}a_1a_2 \quad a_{\phi(m)} \bmod m$, and so by the same corollary, $a^{\phi(m)} \equiv 1 \bmod m$. ■

Corollary 19.3. (Fermat's Theorem) $a, p \in Z$, $p > 0$, p a prime, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \bmod p$.

Corollary 19.4. $a, p \in Z$, $p > 0$, p a prime $\Rightarrow a^p \equiv a \bmod p$.

Definition 19.5. $a \in Z$, a is *even* $\Leftrightarrow 2|a$; a is *odd* $\Leftrightarrow 2 \nmid a$.

Problem 19.10. Prove Corollary 19.3 directly.

Problem 19.11. Give three examples in which the cancellation law of multiplication does not hold in Z_m, for some $m \in Z$.

Problem 19.12. Prove: the nonzero elements of Z_m and the multiplication induced in Z_m by that in Z form a group $\Leftrightarrow m$ is a prime.

Problem 19.13. Prove that the reduced residue classes of Z_m and multiplication form a group.

Problem 19.14. Show that Z_4 and addition is a group which is not isomorphic to the reduced residue classes of Z_8 and multiplication. Find groups previously studied which are isomorphic to each.

Problem 19.15. Show that Z_6 and addition is isomorphic to the reduced residue classes of Z_7 and multiplication.

Problem 19.16. Find all isomorphisms of the groups of Problem 19.15.

Problem 19.17. Show that the even integers of Z and addition form a group isomorphic to the additive group of Z.

Problem 19.18. Find an explicit formula giving one or more integers $x \ni ax \equiv b \bmod m$ and state when it is valid.

Chapter 3: Groups

This chapter is devoted to the study of groups. Most of it concerns the application to groups of a large number of the fundamental concepts discussed in the first two chapters. We consider subsystems (called subgroups), naming the various types, and we combine one type with equivalence relations to obtain the concept of a quotient group. We introduce free groups as another way of obtaining groups with a few generators and a few generating relations.

A discussion of abelian groups of finite order is included for two reasons. The subject is of considerable importance for other matters and also it provides a neat example of a mathematical problem completely solved.

Two Sylow theorems are established and a few applications of them are given to illustrate briefly the problems involved in the study of groups of finite order.

Permutation groups are considered for their own importance and for their use in Chapter 6 in considering the Galois Theory of Equations.

Automorphisms and endomorphisms of some groups of small finite order are considered to illustrate part of the general theory and to lead to the consideration of rings in Chapter 4.

Finally, composition series are considered and the fundamental theorem about them for finite groups is proved to have it available for Chapter 6.

1 GENERAL PROPERTIES OF SUBGROUPS

We have previously given in Definitions 4.2 and 6.2 of Chapter 2 the definitions of subsemigroups and subgroups. We now consider various of their properties and distinguish between some different kinds of subgroups.

DEFINITION 1.1. If G is a group, the two subgroups of G consisting respectively of G itself and of the neutral element alone are called *improper subgroups*. All other subgroups of G are called *proper subgroups*.

THEOREM 1.1. Let $\langle G, \square \rangle$ be a group and H a set of elements of G. Then,

(1) H and $\square$ form a subsemigroup of $G \Leftrightarrow$ condition (1) of Definition 6.1b of Chapter 2 holds:

(2) H and $\square$ form a subgroup of $G \Leftrightarrow$ conditions (1), (3), and (4) of Definition 6.1b of Chapter 2 hold:

(3) if G is finite, H and $\square$ form a subgroup of $G \Leftrightarrow$ condition (1) of Definition 6.1b of Chapter 2 holds.

PROOF: The first two statements follow from the condition that $\square$ is associative in G and so in H; the third follows from Theorem 6.1 of Chapter 2.

PROBLEM 1.1. Find all subgroups of S_3 (cf. Problem 4.2 of Chapter 2).

PROBLEM 1.2. Find all subgroups of the additive group of Z.

PROBLEM 1.3. Find all the subgroups of $\langle Z_7, + \rangle$; $\langle Z_8, + \rangle$; $\langle Z_{21}, + \rangle$.

PROBLEM 1.4. Find all subgroups of the reduced residue classes of Z_{10} and $\cdot$, Z_8 and $\cdot$, Z_5 and $\cdot$.

PROBLEM 1.5. Prove that if H is a finite subset of a group $\langle G, \square \rangle$, and if H is closed with respect to $\square$, then $\langle H, \square \rangle$ is a subgroup of $\langle G, \square \rangle$.

THEOREM 1.2. If H and K are subgroups (subsemigroups with $H \cap K \neq \varnothing$) of a group (semigroup) G, then $H \cap K$ is a subgroup (subsemigioup) of G.

The remark at the end of Section 4 of Chapter 2 about omitting mention of the law of composition of a group is followed in stating the above theorem.

PROBLEM 1.6. Prove Theorem 1.2.

PROBLEM 1.7. Give an example to show that a theorem about $H \cup K$, similar to Theorem 1.2, does not, in general, hold.

PROBLEM 1.8. Generalize Theorem 1.2 to any collection of subgioups of a gioup. Prove your generalization.

Due to the situation that the union of subgroups is not necessarily a subgroup we must resoit to a different method of finding a subgroup containing two given subgroups. Some aspects of the method are useful generally, so we give a very general definition.

Definition 1.2. Given a set S and a property P (which may have several conditions to be fulfilled). The *smallest subset of S possessing the property P* is that subset T of S, if one exists, which satisfies

(1) T has the property P

(2) $\forall\, U \subset S \ni U$ has the property P, $T \subset U$.

Thus, for example, we may speak of the smallest subgroup of a group G, i.e., the smallest subset of G which has the property of being a group (with the same law of composition as G, of course). Here, the subset clearly exists: it is the subgroup consisting of the neutral element alone. However, we could also ask to find the smallest subgroup of G which contains all the elements of a particular subset H of G. We can obtain the smallest subsemigroup with this property as follows. Consider all products (to use multiplication as the law of composition) of a finite number of elements of H: $\prod_{i=1}^{n} h_i$. Taking two such $\prod_{i=1}^{n} h_i$ and $\prod_{i=n+1}^{m} h_i$ and multiplying them we get $\prod_{i=1}^{m} h_i$, which is also a product of a finite number of elements of H. That the associative law holds for such products follows from Theorem 3.1 of Chapter 2. Thus we have a subsemigroup which contains H (since of course n or m or both can be 1). Furthermore, any subsemigroup which contains all the elements of H must contain this subsemigroup. Therefore, by Definition 1.2, it is the smallest subsemigroup of G which contains H. Thus we have proved:

Theorem 1.3. The smallest subsemigroup of a semigroup S containing a nonempty subset H of S is the set of all composites of a finite nonzero number of elements of H.

It should be noted that if S has a neutral element, then the conditions that H be nonempty and nonzero may be dropped. This is a simple consequence of Definition 15.1 of Chapter 2. The next three theorems can be proved after the manner of Theorem 1.3.

Theorem 1.4. The smallest subsemigroup of a semigroup S containing a nonempty subset H of S is the common part of all subsemigroups of G containing H.

Theorem 1.5. The smallest subgroup of a group G containing a subset H of G, is the set of all composites of a finite number of elements of H and inverses of elements of H.

Theorem 1.6. The smallest subgroup of a group G containing a subset H of G is the common part of all subgroups of G containing H.

Problem 1.9. Prove Theorems 1.4, 1.5, and 1.6.

The above four theorems are fairly simple consequences of the definitions of subsemigroup and subgroup. The next theorem is less obvious and is a result which we shall often find very useful.

THEOREM 1.7. Let H be a nonempty subset of a group $\langle G, \square \rangle$. Then H and the restriction of $\square$ to H form a subgroup of $G \Leftrightarrow a \square b^{-1} \in H$ whenever $a, b \in H \Leftrightarrow b^{-1} \square a \in H$ whenever $a, b \in H$.

PROOF: We shall prove the first necessary and sufficient condition and leave the other to the reader.

The implication "$\Rightarrow$" is obvious.

Consider the implication "$\Leftarrow$". Suppose $a \square b^{-1} \in H$ whenever $a, b \in H$. Then in particular, $a \square a^{-1} = e \in H$, where e is the neutral element of G, and $e \square a^{-1} = a^{-1} \in H$, $\forall\ a \in H$. Thus conditions (3) and (4) of Definition 6.1b of Chapter 2 are satisfied. We have just established that $b \in H \Rightarrow b^{-1} \in H$. Therefore, $\forall\ a, b \in H$, $a \square b = a \square (b^{-1})^{-1} \in H$ and so condition (1) of that same definition is satisfied. Therefore, by Theorem 1.1, part (2), H is a subgroup of G. ∎

2. CYCLIC GROUPS AND SUBGROUPS

This section will be devoted primarily to a particularly elementary type of group, but first we make a definition which introduces a more general concept.

DEFINITION 2.1. (a) The subsemigroup (subgroup) whose existence is established by Theorem 1.3 (Theorem 1.5) is called the subsemigroup (subgroup) generated by the set H.

(b) A set of elements H is a *set of generators* of the subsemigroup (subgroup), K, of a semigroup S (group G) $\Leftrightarrow$ K is the subsemigroup of S (subgroup of G) generated by the set H.

(c) A subgroup K of a group G is a *cyclic subgroup* of G $\Leftrightarrow$ K is generated by a set H consisting of a single element, which is then called a *generator* of the cyclic subgroup. In this case, if $K = G$, we say that G is a *cyclic group*.

Of course, in all three parts of the above definition, the whole group or semigroup may be the subgroup or subsemigroup.

PROBLEM 2.1. Prove directly, by using Theorem 15.1 of Chapter 2, that the set of all powers (cf. Definitions 15.5 and 3.3 of Chapter 2) of a single element $a \in G$, a group, form a subgroup of G.

PROBLEM 2.2. Give five cyclic groups considered so far.

Problem 2.3 Prove that $(a^{-1})^{-1} = a$ in a semigroup with a neutral element. Do it without using Theorem 15.1 of Chapter 2.

Problem 2.4 Prove that

$$\iota = \begin{pmatrix} abcd \\ abcd \end{pmatrix} \quad \alpha = \begin{pmatrix} abcd \\ bcda \end{pmatrix} \quad \beta = \begin{pmatrix} abcd \\ cdab \end{pmatrix} \quad \gamma = \begin{pmatrix} abcd \\ dabc \end{pmatrix}$$

form a cyclic group. Show that α and γ are generators but that ι and β are not.

Problem 2.5 Prove that

$$\iota = \begin{pmatrix} abcd \\ abcd \end{pmatrix} \quad \delta = \begin{pmatrix} abcd \\ badc \end{pmatrix} \quad \epsilon = \begin{pmatrix} abcd \\ cdab \end{pmatrix} \quad \eta = \begin{pmatrix} abcd \\ dcba \end{pmatrix}$$

form a group which is not cyclic.

Problem 2.6 Give all the elements of the cyclic group generated by $\lambda = \begin{pmatrix} abcde \\ bcdea \end{pmatrix}$. Which are generators?

Problem 2.7 Prove every subgroup of a cyclic group is cyclic.

Definition 2.2 The order of the cyclic subgroup generated by an element $a \in G$, a group, is called the *period* of a. (It is frequently also called the *order* of a.)

Problem 2.8 Prove that $\alpha = \begin{pmatrix} a_1 a_2 \cdots a_{n-1} a_n \\ a_2 a_3 \cdots a_n \; a_1 \end{pmatrix}$ is of period n. Thus prove that there exists a cyclic group of order n for each positive integer n.

Problem 2.9 Prove that two cyclic groups of the same order are isomorphic.

Theorem 2.1 If the finite cyclic subgroup H of the group G generated by the element a is of order n, then H consists of the elements $a, a^2, \ldots, a^n = e$, where e is the neutral element of G.

Proof Since H is finite, the elements a^i, $i \in N$, cannot all be different. Let $a^k = a^h$, where for definiteness we may suppose that $k < h$. Then $e = a^{h-k}$, where $h - k > 0$.

Then we know that the set $L = \{x | x \in N, a^x = e\}$ is nonempty and so there exists a smallest element in it, say m. Then $a^m = e$. For $0 < s < t < m$, $a^s \neq a^t$, since if $a^s = a^t$, then $a^{t-s} = e$ and $0 < t - s$

$< m$, and this is impossible since m was the smallest element of L. Thus $a, a^2, a^3, \ldots, a^{m-1}, e$ are all distinct.

Every element of H is one of these m elements, since $\forall\, w \in Z$, by Theorem 17.1 of Chapter 2, $\exists\, q, r \in Z \ni w = mq + r$, with $0 < r < m$ and $a^w = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r = e^q a^r = ea^r = a^r$. Therefore, $m = n$. ■

THEOREM 2.2. If G is a cyclic group of finite order n, generated by a, then the number of distinct generators of G is $\phi(n)$, and the generators are the elements a^k, where $k \in Z$ and $(k, n) = 1$.

PROOF: Let $k \in Z$ and let $(k, n) = 1$. To show that a^k is a generator of G, it suffices to show that $(a^k)^h, h = 1, 2, \ldots, n$, are distinct, since there are only n elements in G.

First, we shall show that $(a^k)^h \neq e$ for $0 < h < n$. For, suppose that $(a^k)^h = e$ for some $h_1, 0 < h_1 < n$. Then $\exists\, q, r \in Z \ni kh_1 = nq + r, 0 < r < n$, [$r > 0$ since $(n, k) = 1$]. Then $e = (a^k)^{h_1} = a^{kh_1} = a^{nq}a^r = a^r$, which is impossible since then there would be fewer than n elements in G.

Now if $(a^k)^s = (a^k)^t$, where $0 < s < t < n$, then $(a^k)^{t-s} = e$, with $0 < t - s < n$, which is impossible by what we have just proved. Therefore, the $(a^k)^h$, $h = 1, 2, \ldots, n$, are all distinct and so a^k generates G.

If $(k, n) = d > 1$, then $(a^k)^{n/d} = (a^k)^{n/(k,n)} = a^{kn/(k,n)} = (a^n)^{k/(k,n)} = e$, and so, in this case, a^k cannot be a generator.

For any $k \in Z \ni (k, n) = 1\ \exists\, k_0 \equiv k \bmod n$, $0 < k_0 < n$ and $a^k = a^{k_0}$. Therefore, the number of distinct generators is the number of positive integers less than n and prime to n. Therefore, there are exactly $\phi(n)$ generators. ■

PROBLEM 2.10. Prove that the period of an element $a \in G$, a group, is the smallest positive integer $n \ni a^n = e$, if there exists such an n.

PROBLEM 2.11. Prove that if n is the period of $a \in G$, a group, and if $a^k = e$, then $n | k$.

PROBLEM 2.12. Prove that if the group G is isomorphic to the group G', and if in that isomorphism $a \in G$ is mapped onto $a' \in G'$, then a and a' have the same period.

PROBLEM 2.13. Investigate the situation of Problem 2.12 in the case where G is merely homomorphic to G'.

PROBLEM 2.14. Prove that if $a, b \in G$, a group, and $ba = ab$

then the period of ab divides the l.c.m. of the periods of a and b.

Problem 2.15 Given $a \in G$, a group, a is of period n and $k \in Z^*$, prove $(k, n) = d \Rightarrow a^k$ is of period $n/(k, n)$.

3. EQUIVALENCE RELATIONS IN A GROUP

The number of equivalence relations which can be defined in a group is rather large since any partition of the set of elements of the group defines an equivalence relation by Theorem 8.2 of Chapter 2. However, the most interesting and useful equivalence relations in any algebraic system are those which are compatible, at least on one side, with the law or laws of composition of the system. It is of considerable importance that we can characterize such equivalence relations completely for a group. We do so in the next two theorems.

Theorem 3.1 If H is a subgroup of a group $(G, \square)$, then $xRy \Leftrightarrow x \square y^{-1} \in H$ ($x^{-1} \square y \in H$) is an equivalence relation compatible on the right (left) with $\square$.

Proof First, we note that since G is a group, $\forall x, y \in G$ either xRy or $x \not R y$, so R is defined for every pair of elements of G.

Next, we prove that R is an equivalence relation.

It is reflexive. For since H is a group, $e \in H$ and so $x \square x^{-1} \in H \Rightarrow xRx$.

It is symmetric. For since H is a group, if $x \square y^{-1} \in H$ (i.e., if xRy), then its inverse $(x \square y^{-1})^{-1} = y \square x^{-1} \in H$, i.e., yRx.

It is transitive. For since H is a group, if $x \square y^{-1} \in H$ and $y \square z^{-1} \in H$ (i.e., if xRy and yRz), then their composite $(x \square y^{-1}) \square (y \square z^{-1}) = x \square z^{-1} \in H$. That is, xRz. Therefore R is an equivalence relation.

Now we prove the right compatibility. If $z \in G$ and $x \square y^{-1} \in H$ (i.e., xRy), then $(x \square z) \square (y \square z)^{-1} = (x \square z) \square (z^{-1} \square y^{-1}) = x \square y^{-1} \in H$, and so $xRy \Rightarrow (x \square z)R(y \square z)$, $\forall z \in G$. We leave the left cases to the reader as an exercise. ■

It should be noted that $hRe \Leftrightarrow h \in H$.

Problem 3.1 Carry through the details of the proof of Theorem 3.1 for the case in parentheses.

Now we prove that the relations discussed in Theorem 3.1 are the only ones compatible on the right or left with the law of composition of the group.

Theorem 3.2 If the relation R is an equivalence relation defined in a group $(G, \square)$ compatible on the right (left) with $\square$, then

(1) the elements $a \in G \ni aRe$ form a subgroup H of G,
(2) R can be defined by $xRy \Leftrightarrow x \square y^{-1} \in H$ $(x^{-1} \square y \in H)$.

PROOF: (1) Let aRe, bRe. By symmetry of R, eRb, and by transitivity, aRb. Then by right compatibility, $a \square b^{-1}Re$, and so by Theorem 1.7, H is a subgroup of G.

(2) The relation $\Rightarrow$. If xRy, then by right compatibility, we have $x \square y^{-1}Re$ and so $x \square y^{-1} \in H$.

The relation $\Leftarrow$. If $x \square y^{-1} \in H$, then by definition of H. $x \square y^{-1}$ Re and by right compatibility, xRy. ■

PROBLEM 3.2. Carry through the details of the proof of Theorem 3.2 for the case in parentheses.

We now introduce a law of composition (in the set of all subsets of a set) which we shall use at present for subsets of a group, but we shall give a definition valid more generally.

DEFINITION 3.1. Let S be a set with a law of internal composition, $\square$, and let H, K be subsets of S. Then $H \square K$ is the set of all elements $h \square k$ where $h \in H$ and $k \in K$.

We shall use the above definition in the next theorem. We need one more definition. It happens that in a group, equivalence classes can be represented in a very simple and convenient form. We introduce terminology for that now.

DEFINITION 3.2. If $\langle H, \square \rangle$ is a subgroup of a group, $\langle G, \square \rangle$, and if R is one of the equivalence relations of Theorem 3.1, then the equivalence classes determined by R are called *right* or *left cosets of G with respect to H* (sometimes briefly, cosets of H if the meaning is clear from the context) according as R is $xRy \Leftrightarrow x \square y^{-1} \in H$ or $xRy \Leftrightarrow x^{-1} \square y \in H$. The number of right cosets is called the *index of H in G* and is denoted by $(G : H)$.

THEOREM 3.3. If H is any subgroup of a group, $\langle G, \square \rangle$, then the right (left) cosets of G with respect to H are the sets $H \square x$ $(y \square H)$, where we have written $H \square x$ as an abbreviation for $H \square \{x\}$, where $x \in G$ $(y \in G)$, and those cosets different from H can be written $H \square x$ $(y \square H)$, where $x \notin H$ $(y \notin H)$.

PROOF: Let $x \in A$, a right coset. Then if $z \in A$, $x \square z^{-1} \in H$, i.e., $x \square z^{-1} = h \in H$, or $x = h \square z$. Therefore, $A \subset H \square x$.

On the other hand, if $z \in H \square x$, then $z = h' \square x$, where $h' \in H$; thus $x = h'' \square z$, where $h'' = h'^{-1} \in H$, so $x \square z^{-1} = h'' \in H$. Therefore, $H \square x \subset A$. Therefore, $H \square x = A$. ■

Problem 3.3 Show that in Z, $a \equiv b \bmod m$ is an equivalence relation of the type of Theorem 3.1.

Problem 3.4 In S_3, let $K_1 = \{\iota, \alpha, \beta\}$. Find αK_1, δK_1, ϵK_1, $K_1\beta$, $K_1\epsilon$.

Problem 3.5 In S_3, let $K_2 = \{\iota, \gamma\}$. Find all right and left cosets of S_3 with respect to K_2.

Problem 3.6 In C_{12}, the cyclic group of order 12 generated by a, let $H = \{1, a^3, a^6, a^9\}$, where $a^{12} = 1$, the neutral element; find aH, a^2H, a^3H.

Problem 3.7 In C_{12} of Problem 3.6, find $(aH)(aH)$, $(aH)(a^2H)$, $H(aH)$, and $(aH)(a^3H)$.

Problem 3.8 Prove: if H is a subset of the finite group $(G, \square)$, then $H \square H = H \Leftrightarrow H$ is a subgroup of G; that for any group the implication "$\Leftarrow$" holds.

Problem 3.9 Prove $(H \square K) \square L = H \square (K \square L)$ for any subsets H, K, L of a semigroup.

Problem 3.10 Prove $h \square H = H$ if H is a subgroup of a group G and $h \in H$.

Problem 3.11 Prove: $a, b \in (G, \square)$, a group, $(H, \square)$ is a subgroup of $(G, \square)$, $b \in a \square H \Rightarrow a \square H = b \square H$.

Problem 3.12 In $(Z, +)$ find the cosets with respect to the subgroups consisting of all integers which are multiples of 5; of m.

Theorem 3.4 A, B are any two cosets of a group G with respect to a subgroup H of $G \Rightarrow \exists$ a 1-1 mapping of A onto B.

Corollary 3.1 The number of elements in any two cosets of a group G with respect to a subgroup H is the same.

Corollary 3.2 The number of left cosets of G with respect to H is equal to the number of right cosets of G with respect to H.

Problem 3.13 Prove Theorem 3.4 and its corollaries.

Theorem 3.5 (Lagrange) If H is a subgroup of a finite group G, then the order of H divides the order of G.

Proof. Let h be the order of H, g the order of G, and k the number of cosets of G with respect to H. By Theorem 8.1 of Chapter 2, every element of G is in one and only one coset. By Corollary 3.1

to Theorem 3.4, each coset has h elements in it. Therefore, the number of elements in G is hk. That is, $g = hk$ and so $h|g$. ■

Corollary 3.3. If H is a subgroup of a finite group G, then the order of G is the product of the order of H and the index of H in G.

Problem 3.14. Prove: G, a group, has order p, a positive prime $\Rightarrow G$ has no proper subgroup.

Problem 3.15. Prove: $k|n \Rightarrow \exists$ a subgroup of order k in the cyclic group of order n.

Problem 3.16. Prove: all groups of order p, a positive prime, are isomorphic.

Problem 3.17. Find the indices of the subgroups in Problems 3.4, 3.5, and 3.6.

Problem 3.18. Prove: H, K are subgroups of a group G, $K \subset H$, $(G:K)$ is finite $\Rightarrow (H:K)$ is finite and $(G:K) = (G:H)(H:K)$.

Problem 3.19. Prove: H, K are subgroups of a group G, $K \subset H$, $(G.H)$ and $(H:K)$ are finite $\Rightarrow (G:K)$ is finite and $(G:K) = (G:H)(H:K)$.

Using the result of Problem 3.5, we see that S_3 can be represented as the union of right cosets as $S_3 = \{\iota, \gamma\} \cup \{\alpha, \epsilon\} \cup \{\beta, \delta\}$, while as the union of left cosets we have $S_3 = \{\iota, \gamma\} \cup \{\alpha, \delta\} \cup \{\beta, \epsilon\}$. If we use the subgroup K_1 of Problem 3.4, the two corresponding representations are the same. It is important to distinguish between such subgroups. The distinction is given by the problem of determining when the equivalence relation determined by a subgroup is compatible (on both sides) with the law of composition of the group. The next two theorems give the complete determination.

Theorem 3.6. If an equivalence relation R defined in a group $\langle G, \Box\rangle$ is compatible with $\Box$, then the subgroup, $H = \{h | h \in G, hRe\}$ has the property that $\forall\, h \in H, \forall\, y \in G, y^{-1} \Box h \Box y \in H$.

Proof: Since R is an equivalence relation, compatibility is equivalent to simultaneous right and left compatibility. Let $h \in H$ and $y \in G$. Let $x = h \Box y$. Then $x \Box y^{-1} = h$ and so by the definition of H, $x \Box y^{-1} Re$, and so by right compatibility, xRy. Now by left compatibility, $eRx^{-1} \Box y$, so $x^{-1} \Box y \in H$, i.e., $y^{-1} \Box x = h_1 \in H$. or $x = y \Box h_1$. Finally, $y \Box h_1 = h \Box y \Rightarrow h_1 = y^{-1} \Box h \Box y$. ■

THEOREM 3.7. If $(H, \square)$ is a subgroup of $(G, \square)$, a group, and if H has the property that $\forall h \in H, \forall y \in G, y^{-1} \square h \square y \in H$, then the equivalence relation of Theorem 3.1 defined by H is compatible with $\square$.

PROOF. We shall prove that the two relations of Theorem 3.1 are equivalent. Let $x \square y^{-1} = h \in H$. Then $x = h \square y$. Since H is a group and $h \in H$, $h^{-1} \in H$, and by hypothesis $y^{-1} \square h^{-1} \square y = h_1 \in H$. Then $x^{-1} \square x = (h \square y)^{-1} \square y = y^{-1} \square h^{-1} \square y = h_1$. Therefore $x \square y^{-1} \in H \Rightarrow x^{-1} \square y \in H$. Similarly $x^{-1} \square y \in H \Rightarrow x \square y^{-1} \in H$.

Thus, since whenever either relation holds the other one does and one is compatible on the right, the other on the left, the single relation is compatible. ■

DEFINITION 3.3. In a group $(G, \square)$ a subgroup H is called *invariant* (*normal* or *self-conjugate*) $\Leftrightarrow \forall h \in H, \forall x \in G, x^{-1} \square h \square x \in H$.

PROBLEM 3.20. Prove: if H is a subgroup of a group $(G, \square)$, then H is invariant $\Leftrightarrow x^{-1} \square H \square x = H, \forall x \in G \Leftrightarrow x \square H = H \square x, \forall x \in G$.

PROBLEM 3.21. Prove that for an invariant subgroup, left cosets are right cosets.

PROBLEM 3.22. Find ten invariant subgroups of groups considered previously.

PROBLEM 3.23. Find three subgroups of the groups considered previously which are not invariant.

PROBLEM 3.24. Prove that a subgroup of index 2 is invariant.

Since we now have an equivalence relation defined in a group $(G, \square)$ and compatible with $\square$, it is natural to consider the quotient set K of G with respect to that relation and the law of composition induced by $\square$ in K. By Theorem 12.1 and Theorem 12.2 of Chapter 2, K is a semigroup. By Theorem 3.3 and the last part of Problem 3.20 and Problem 3.9, we have $H \square (a \square H) = (H \square a) \square H = (a \square H) \square H = a \square (H \square H) = a \square H$ and similarly $(a \square h) \square H = a \square H$. (We have used $\square$ for the induced law, but by Theorem 3.3 there is no danger of confusion.) Thus H is a neutral element for K. Finally, by similar reasoning $(a^{-1} \square H) \square (a \square H) = H = (a \square H) \square (a^{-1} \square H)$, so every element of K has an inverse in K. Therefore K is a group and we have proved

THEOREM 3.8. Let $\langle G, \Box \rangle$ be a group and H an invariant subgroup of G. Let R be the equivalence relation of Theorem 3.1. Then the quotient set G/R and the law of composition induced by $\Box$ in G/R is a group, called the *quotient group of G with respect to H* and is denoted by G/H. (This is sometimes called a *factor group*.)

PROBLEM 3.25. Find the quotient groups of C_{12} (cf. Problem 3.6) with respect to two of its proper subgroups.

PROBLEM 3.26. Find the quotient group of S_3 with respect to its proper invariant subgroup (cf. discussion preceding Theorem 3.6).

DEFINITION 3.4. A group is *abelian* (or *commutative*) $\Leftrightarrow$ its law of composition is commutative.

PROBLEM 3.27. Find six abelian groups so far considered.

PROBLEM 3.28. Prove that any quotient group of an abelian group is abelian.

PROBLEM 3.29. Prove that any quotient group of a cyclic group is cyclic.

4. HOMOMORPHISMS AND ISOMORPHISMS OF GROUPS

Homomorphic mappings of algebraic systems in general are of the utmost importance in most of the study of algebra. The most basic result for groups is the next theorem.

THEOREM 4.1. Let α be a homomorphic mapping of a group $\langle G, \Box \rangle$ into a set E which possesses a law of internal composition $\bigcirc$. Then

(1) the set of images, $K = G\alpha$, and $\bigcirc$ form a group,

(2) the set $H = \{x | x \in G, x\alpha = e'\}$ and $\Box$, where e' is the neutral element of K, is an invariant subgroup of G, called the *kernel of* α.

(3) G/H is isomorphic to K.

PROOF: (1) Let $k_1, k_2 \in K$. Then $\exists\, g_1, g_2 \in G \ni g_1\alpha = k_1$, $g_2\alpha = k_2$. Now, since G is closed under $\Box$, $\exists\, g_3 \in G \ni g_3 = g_1 \Box g_2$, and so $\exists\, k_3 \in K \ni g_3\alpha = k_3$. Then $k_3 = g_3\alpha = (g_1 \Box g_2)\alpha = (g_1\alpha) \bigcirc (g_2\alpha) = k_1 \bigcirc k_2$. Therefore, K is closed under $\bigcirc$.

Let $k_1, k_2, k_3 \in K$. Then $\exists\, g_1, g_2, g_3 \in G \ni g_1\alpha = k_1$, $g_2\alpha = k_2$, $g_3\alpha = k_3$. $k_1 \bigcirc (k_2 \bigcirc k_3) = (g_1\alpha) \bigcirc [(g_2\alpha) \bigcirc (g_3\alpha)] = (g_1\alpha) \bigcirc [(g_2 \Box g_3)\alpha] = [g_1 \Box (g_2 \Box g_3)]\alpha = [(g_1 \Box g_2) \Box g_3]\alpha = [(g_1 \Box g_2)\alpha] \bigcirc (g_3\alpha) = [(g_1\alpha) \bigcirc (g_2\alpha)] \bigcirc (g_3\alpha) = (k_1 \bigcirc k_2) \bigcirc k_3$. Therefore, the law of composition $\bigcirc$ is associative in K.

Since G is a group G has a neutral element e Let $e' = e\alpha$ and let $k \in K$ Then $\exists g \in G \ni g\alpha = k$ Then $e' \bigcirc k = (e\alpha) \bigcirc (g\alpha) = (e \square g)\alpha = g\alpha = k$ Similarly $k \bigcirc e' = k$ Therefore e' is a neutral element for K

Let $k \in K$ and let $g \in G \ni g\alpha = k$ Then $\exists g^{-1} \in G$ and $\exists k' \in K \ni k' = g^{-1}\alpha$ Then $k \bigcirc k' = (g\alpha) \bigcirc (g^{-1}\alpha) = (g \square g^{-1})\alpha = e\alpha = e'$ Similarly $k' \bigcirc k = e'$ Therefore k' is the inverse of k and so K is a group

(2) Let $g_1, g_2 \in G$ be $\ni g_1\alpha = e'$, $g_2\alpha = e'$ Then $e' = e\alpha = (g_2 \square g_2^{-1})\alpha = (g_2\alpha) \bigcirc (g_2^{-1}\alpha) = g_2^{-1}\alpha$ Therefore $(g_1 \square g_2^{-1})\alpha = e'$ Therefore by Theorem 1 7 H is a subgroup of G Let $h \in H$ and $g \in G$ Then $(g^{-1} \square h \square g) = (g^{-1}\alpha) \bigcirc (h\alpha) \bigcirc (g\alpha) = (g^{-1}\alpha) \bigcirc e' \bigcirc (g\alpha) = (g^{-1}\alpha) \bigcirc (g\alpha) = (g^{-1} \square g)\alpha = e\alpha = e'$ Therefore $h \in H \Rightarrow g^{-1} \square h \square g \in H \; \forall g \in G$ Therefore by Definition 3 3 H is an invariant subgroup of G

(3) The quotient group G/H consists of cosets of G with respect to H We must show first that there exists a 1 1 mapping of these cosets onto K The mapping α will give us the desired mapping Let A be any coset and let $a_1, a_2 \in A$ Then $A = a \square H = H \square a$ by Theorem 3 3 and Definition 3 3 so $a_1 = a \square h_1$, $a_2 = a \square h_2$ where $h_1, h_2 \in H$ Then $a_1\alpha = (a \square h_1)\alpha = (a\alpha) \bigcirc (h_1\alpha) = (a\alpha) \bigcirc e' = a\alpha$ and similarly $a_2\alpha = a\alpha$ Therefore under α all elements of A are mapped onto the same element of K so without danger of confusion we may write $A\alpha = a\alpha$ though this is an extension of the meaning of the mapping α We then have a mapping of G/H into K It is onto since if $k \in K$ $\exists g \in G \ni g\alpha = k$ and so $(g \square H)\alpha = k$ It is 1 1 since if $A\alpha = B\alpha$ letting $a \in A$, $b \in B$ then we have $a\alpha = b\alpha \Rightarrow a^{-1}\alpha = b^{-1}\alpha \Rightarrow (a \square b^{-1})\alpha = (a\alpha) \bigcirc (b^{-1}\alpha) = (a\alpha) \bigcirc (a^{-1}\alpha) = (a \square a^{-1})\alpha = e\alpha = e' \Rightarrow a \square b^{-1} \in H \Rightarrow (a, b \in A$ and $a, b \in B) \Rightarrow A = B$

Lastly letting $a, b \in$ two cosets A, B respectively and letting C be the coset containing $c = a \square b$ we have $(A \square B)\alpha = C\alpha = c\alpha = (a \square b)\alpha = (a\alpha) \bigcirc (b\alpha) = A\alpha \bigcirc B\alpha$ which establishes the homomorphism ∎

PROBLEM 4 1 The following mapping α is an endomorphism (cf Definition 11 1 of Chapter 2) of the cyclic group C_{12} of order 12 generated by a a^{4k} $\alpha = (a^3)$ for $j = 1, 2, 3, 4$ and $\forall k \in Z^*$ Find $C_{12}\alpha$ and the kernel H of α Discuss C_{12}/H

PROBLEM 4 2 Find a homomorphism of S_3 onto the cyclic group of order 2 Find the kernel

Problem 4.3. Find all other possible homomorphisms of S_3. (Hint: for each homomorphism, there must be an invariant subgroup.)

Theorem 4.2. *H is an invariant subgroup of the group $\langle G, \square\rangle$ $\Rightarrow$ the mapping, α, defined by $x\alpha = x \square H$, $\forall\, x \in x \square H$ (i.e., each element is mapped onto the coset to which it belongs), is a homomorphism of G onto G/H. This homomorphism is called the* canonical *(also* natural*) homomorphism of G onto G/H.*

Problem 4.4. Prove Theorem 4.2. (Hint: use the proof of the preceding theorem.)

Problem 4.5. Write out in full detail the canonical homomorphism of C_{12} of Problem 4.1 onto C_{12}/H, where $H = \{1, a^4, a^8\}$, where 1 is the neutral element.

Problem 4.6. For H and C_{12} as in Problem 4.5, give another homomorphism of C_{12} onto C_{12}/H.

Theorem 4.3. *$a \in G$, a group $\Rightarrow$ the mapping $g\alpha = a^{-1} \square g \square a$, $\forall\, g \in G$, is an automorphism of G.*

Proof: This mapping is 1–1 since if $a^{-1} \square g \square a = a^{-1} \square g' \square a$, then $g \square a = g' \square a$ and $g = g'$, applying the right and left cancellation laws. This mapping is onto since if $h \in G$, $a \square h \square a^{-1} = g \in G$ and $a^{-1} \square g \square a = h$. Lastly, $(g \square h)\alpha = a^{-1} \square (g \square h) \square a = (a^{-1} \square g \square a) \square (a^{-1} \square h \square a) = g\alpha \square h\alpha$. Therefore, α is an automorphism of G. ■

Definition 4.1. An automorphism of a group G, which can be determined by a single element of G, as in Theorem 4.3, is called an *inner automorphism*. All other automorphisms of G are called *outer automorphisms*.

Problem 4.7. Prove: H, a subgroup of G, is an invariant subgroup of $G \Leftrightarrow H$ is mapped onto itself by every inner automorphism of G.

Problem 4.8. Prove: an abelian group has exactly one inner automorphism.

Problem 4.9. Find all the inner automorphisms of S_3. Show that they form a group.

Problem 4.10. Find the set of all automorphisms of C_{12} and show that they form a group.

PROBLEM 4 11 Prove a cyclic group of order n has exactly $\phi(n)$ automorphisms

PROBLEM 4 12 Find all outer automorphisms of S_3 if any

PROBLEM 4 13 The additive group of Z has a subgroup H_3 consisting of all multiples of three Find Z/H_3

PROBLEM 4 14 Find all subgroups of Z and the quotient groups of Z with respect to each of them

PROBLEM 4 15 Prove $G = S \times T$ where S and T are groups $\Rightarrow$

(1) G has two invariant subgroups one of which is isomorphic to S and the other one is isomorphic to T

(2) G/S is isomorphic to T G/T to S

PROBLEM 4 16 For a group G of finite order g and invariant subgroup H of order h prove that the order of G/H is g/h

THEOREM 4 4 Let H be an invariant subgroup of a group $(G \square)$ and let α be the canonical homomorphism of G onto $G/H = G'$ Then

(1) for each subgroup K' of G' the set of all elements $x \in G \ni x\alpha \in K'$ is a subgroup of G which contains H

(2) the mapping of conclusion (1) is a 1 1 mapping of the set of subgroups of G' onto the set of subgroups of G containing H

(3) if K' is an invariant subgroup of G' the corresponding subgroup K of G is an invariant subgroup of G and G'/K' is isomorphic to G/K

(4) for any subgroup L of G $L/(H \cap L)$ is isomorphic to $(H \square L)/L$

PROOF We shall leave the proof of statements (1) and (2) to the reader as an exercise and we shall now prove (3) and (4)

(3) Let β be the canonical homomorphism of G' onto G'/K' Then $\alpha\beta$ is a homomorphism of G onto G'/K' The kernel of $\alpha\beta$ is the set of elements of G mapped into K' under α This set of elements by conclusion (1) is denoted by K and so by Theorem 4 1 (2) it is an invariant subgroup of G Therefore by Theorem 4 1 (3) G/K is isomorphic to G'/K'

(4) Since H is invariant in G $H \square L$ is a subgroup of G and H is an invariant subgroup of $H \square L$ Every coset of $H \square L$ with respect to H has elements in L Therefore in the canonical homomorphism of $H \square L$ onto $(H \square L)/L$ the subgroup L is mapped onto $(H \square L)/L$ Therefore by Theorem 4 1 $(H \square L)/L$ is isomorphic to the quotient

group of L with respect to the invariant subgroup consisting of all elements of L which are mapped onto the neutral element. These are precisely the elements of $H \cap L$. Therefore, $(H \Box L)/L$ is isomorphic to $L/(H \cap L)$. ■

PROBLEM 4.17. Complete the proof of Theorem 4.4 by proving statements (1) and (2).

We now consider two subgroups of the group of Theorem 7.1 of Chapter 2.

THEOREM 4.5. The set of all automorphisms of a group $\langle G, \Box\rangle$ is a subgroup of the group of all 1–1 mappings of the set G onto itself.

PROOF: Let α, β be automorphisms of G. We shall show first that β^{-1} is an automorphism of G, where β^{-1} is the inverse of β as a 1–1 mapping of G onto itself. Let $a, b \in G$. Then $(a \Box b)\beta^{-1} \in G$ and $[(a \Box b)\beta^{-1}]\beta = a \Box b$. Also, $[(a\beta^{-1}) \Box (b\beta^{-1})]\beta = (a\beta^{-1})\beta \Box (b\beta^{-1})\beta = a \Box b$, since β is an automorphism. Thus we have $[(a \Box b)\beta^{-1}]\beta = [(a\beta^{-1}) \Box (b\beta^{-1})]\beta$. Hence, since β is a 1–1 mapping, $(a \Box b)\beta^{-1} = (a\beta^{-1}) \Box (b\beta^{-1})$. Therefore, β^{-1} is an automorphism of G. Hence, by Theorem 7.1 of Chapter 2, $\alpha\beta^{-1}$ is a 1–1 mapping of G onto itself.

Then finally, $(a \Box b)(\alpha\beta^{-1}) = [(a\alpha) \Box (b\alpha)]\beta^{-1} = (a\alpha)\beta^{-1} \Box (b\alpha)\beta^{-1} = a(\alpha\beta^{-1}) \Box b(\alpha\beta^{-1})$. Therefore, $\alpha\beta^{-1}$ is an automorphism of G.

Hence, by Theorem 1.7, the set of automorphisms of G is a group. ■

THEOREM 4.6. The set of all inner automorphisms of a group G is an invariant subgroup of the group of all automorphisms of G.

PROBLEM 4.18. Prove Theorem 4.6.

DEFINITION 4.2. Let $\langle G, \Box\rangle$ be a group. The set of all elements $c \in G \ni \forall x \in G, c \Box x = x \Box c$ is called the *central* of G. (Sometimes the *center*.)

PROBLEM 4.19. Prove: the central of a group G is an invariant subgroup of G.

PROBLEM 4.20. Find the central of S_3, and of an abelian group.

THEOREM 4.7. C is the central of a group $G \Longrightarrow$ the group of inner automorphisms of G is isomorphic to G/C.

PROBLEM 4.21. Prove Theorem 4.7. (Hint: apply theorem 4.1.)

PROBLEM 4.22. Apply Theorem 4.7 to find all inner automorphisms of S_3.

5. TWO FAMILIES OF GROUPS

So far we have considered only one finite non-abelian group S_3. We are going to consider next some properties of groups which are of importance only for non-abelian groups. So, in order to have a wider variety of examples illustrating the general theory, we interrupt the development of the theory to consider briefly two families of groups which are, in general, non-abelian. We shall subsequently discuss how to analyze groups in general in the form in which we now give these groups. Let it be assumed at present that there is nothing contradictory about the given relations. In both cases the groups are defined in terms of two generating elements which satisfy the given relations and *no others* except those relations which are implied by the given ones.

Dihedral group of order 2n, D_{2n}. The two generating elements are a and b, and they satisfy $a^2 = 1$, $b^n = 1$, $abab = 1$ (where 1 is the neutral element). This last relation may be written as $ab = b^{-1}a$. A typical case is that of $n = 4$. Here it is easy to show, by using the last defining relation, that every product of a's and b's can be written in one of the eight forms $1, b, b^2, b^3, a, ab, ab^2, ab^3$. (For example, ba can be obtained as follows: from $ab = b^3a$ ($b^{-1} = b^3$ here) we have $bab = b^4a = a$, $ba = ab^3$.) If any two of those eight elements were equal, we should have an additional relation not implied by the given ones.

Quaternion group of order 4n, Q_{4n}. Again we have two generators c, d and the generating relations are $d^{2n} = 1$, $d^nc^{-2} = 1$, $cdc^{-1}d = 1$, or the latter two may be put in somewhat more convenient form as $c^2 = d^n$, $cd = d^{-1}c$. The elements of this group are $1, d, d^2, \ldots, d^{2n-1}$, $c, cd, cd^2, \ldots, cd^{2n-1}$.

PROBLEM 5.1. Show that D_4 is isomorphic to $K_2 \times K_2$ of Problem 9.2 of Chapter 2 and is not isomorphic to Q_4.

PROBLEM 5.2. Show that D_6 is isomorphic to S_3.

PROBLEM 5.3. Write out the composition tables for D_8 and Q_8. Prove that these groups are not isomorphic.

PROBLEM 5.4. Find all subgroups of D_8 and determine which are invariant.

PROBLEM 5.5. Do the same as Problem 5.4 for Q_8.

PROBLEM 5.6. For the invariant subgroups found in Problems 5.4 and 5.5, discuss the corresponding quotient groups.

6. CONJUGATES

Now, as promised, we consider some concepts which are of no importance in abelian groups.

DEFINITION 6.1. Let $\langle G, \Box\rangle$ be a group. Two elements $a, b \in G$ (two subgroups H, K of G) are *conjugates* in $G \Leftrightarrow \exists$ an inner automorphism α of $G \ni a\alpha = b$ $(H\alpha = K)$. The set of all distinct $a\alpha$ $(H\alpha)$, for all inner automorphisms α of G, is called a *complete set of conjugate elements* (subgroups), or more simply, a *complete set of conjugates.*

EXAMPLE 6.1. In S_3, $\alpha^{-1}\gamma\alpha = \beta\gamma\alpha = \delta$, so γ and δ are conjugates. Also, $\beta^{-1}\gamma\beta = \alpha\gamma\beta = \epsilon$, so γ and ϵ are conjugates. Further, $\gamma^{-1}\gamma\gamma = \gamma\gamma\gamma = \gamma$, $\iota^{-1}\gamma\iota = \gamma$, so γ is a conjugate of itself. Finally, $\delta^{-1}\gamma\delta = \delta\gamma\delta = \epsilon$, $\epsilon^{-1}\gamma\epsilon = \epsilon\gamma\epsilon = \delta$, and so, since the images of γ under all inner automorphisms of S_3 have been considered, $\{\gamma, \delta, \epsilon\}$ form a complete set of conjugates of γ.

PROBLEM 6.1. Prove that the relation of being conjugate is an equivalence relation (both for elements and subgroups).

PROBLEM 6.2. Find all the complete sets of conjugates of elements and subgroups in S_3; in D_8; in Q_8.

PROBLEM 6.3. Prove: H is an invariant subgroup of the group $G \Leftrightarrow H$ coincides with all its conjugates (hence the name, self-conjugate).

THEOREM 6.1. Let $\langle G, \Box\rangle$ be a group and $a \in G$. The set $N = \{x | x \in G,\ x \Box a = a \Box x\}$ is a subgroup of G, and if G is a finite group, $(G : N)$ is the number of distinct conjugates of a (including a itself) in G. The subgroup N is called the *normalizer* of a in G.

PROOF: Since $a \in N, N$ is nonempty. Let $x, y \in N$. Since $y \Box a = a \Box y$, upon multiplying on the left by y^{-1}, we have $a = y^{-1} \Box a \Box y$ and then, upon multiplying on the right by y^{-1}, we have $a \Box y^{-1} = y^{-1} \Box a$. Therefore, $y \in N \Rightarrow y^{-1} \in N$. Hence, we have $(x \Box y^{-1}) \Box a = x \Box (y^{-1} \Box a) = x \Box (a \Box y^{-1}) = (x \Box a) \Box y^{-1} = (a \Box x) \Box y^{-1} = a \Box (x \Box y^{-1})$. Therefore, $x, y \in N \Rightarrow x \Box y^{-1} \in N$. Therefore, by Theorem 1.7, N is a subgroup of G.

Let $x \in A, y \in B$, where A and B are right cosets of G with respect to N and suppose that $x^{-1} \Box a \Box x = y^{-1} \Box a \Box y$. Then $a \Box$

$x = x \square y^{-1} \square a \square y$ and so $a \square x \square y^{-1} = x \square y^{-1} \square a$ Therefore $x \square y^{-1} \in N$ and so x y belong to the same right coset Hence if two elements of G provide the same conjugates of a the two elements belong to the same right coset Thus elements belonging to different cosets give different conjugates Hence the number of conjugates is at least equal to the number of cosets However if $x \in N \square z$ $y \in N \square z$ then $x = n_1 \square z$ $y = n_2 \square z$ where n_1 and $n_2 \in N$ and we have $x^{-1} \square a \square x = z^{-1} \square n_1^{-1} \square a \square n_1 \square z = z^{-1} \square a \square z$ and $y^{-1} \square a \square y = z^{-1} \square n_2^{-1} \square a \square n_2 \square z = z^{-1} \square a \square z$ Thus elements belonging to the same right coset give the same conjugate of a Therefore the number of conjugates is $(G\ N)$ ■

COROLLARY 6 1 The number of conjugates of an element $a \in G$ a finite group divides the order of the group

THEOREM 6 2 Let $(G\ \square)$ be a group and H a subgroup of G The set $N = \{x | x \in G\ x \square H = H \square x\}$ is a subgroup of G H is an invariant subgroup of N and if G is a finite group $(G\ N)$ is the number of distinct conjugate subgroups of H in G (including H itself) The subgroup N is called the *normalizer* of H in G

COROLLARY 6 2 The number of subgroups conjugate to a subgroup of a group G divides the order of G

PROBLEM 6 4 Prove Theorem 6 2

PROBLEM 6 5 Prove Corollaries 6 1 and 6 2

PROBLEM 6 6 Find the normalizer of each element in S_3 of a b in D_n of c d in Q_{2n}

PROBLEM 6 7 Prove that the order of the normalizer of a subgroup H is greater than or equal to the order of H

THEOREM 6 3 Let G be a finite group Then no proper subgroup H can contain elements from each of the complete sets of conjugates of elements of G

PROOF Suppose H were such a subgroup and let h be its order and let g be the order of G Let n be the order of the normalizer of H in G Then of course since $N \supset H$ $n \geqslant h$ Now H is one of g/n conjugate subgroups each of order h The neutral element is common to all these conjugate subgroups and in G there is a total of at most $1 + (g/n)\ (h - 1)$ elements Now the maximum value possible for $1 + (g/n)\ (h - 1)$ is g but this only occurs if $n = h = g$ In this case H is not a proper subgroup Otherwise this quantity is less than g

and so the complete set of conjugate subgroups of which H is a member cannot contain all the elements of G. Therefore, there must be additional elements of G, which is impossible. ■

PROBLEM 6.8. Examine S_3, D_8, Q_8 in light of Theorem 6.3.

7. DIRECT PRODUCTS

Let us consider the cyclic group of order 6 generated by its element a. We write it multiplicatively as $G = \{1, a, a^2, a^3, a^4, a^5\}$ where $a^6 = 1$. Let us also consider the following subgroups of G: $H_1 = \{1, a^2, a^4\}$, $H_2 = \{1, a^3\}$. The first subgroup is generated by a^2, the second by a^3. We easily verify that each element of G can be represented as a power of a^2 times a power of a^3 as follows: $a = (a^2)^2(a^3)^1$, $a^2 = (a^2)^1(a^3)^0$, $a^3 = (a^2)^0(a^3)^1$, $a^4 = (a^2)^2(a^3)^0$, $a^5 = (a^2)^1(a^3)^1$, $a^6 = (a^2)^0(a^3)^0 = a^0 = 1$. We leave it to the reader to verify that this representation is unique if we restrict ourselves to using exponents which are nonnegative and less than the period of (a^2) for any exponent placed on (a^2), and less than the period of (a^3) for any of its exponents, and is unique as far as the elements used are concerned. This decomposition of a cyclic group of nonprime order is frequently possible as is established by the following theorem.

THEOREM 7.1. Let $\langle G, \Box\rangle$ be a group and let $z \in G$. Then z is of period mn where $(m, n) = 1$, $m > 1$, $n > 1 \Rightarrow \exists\, x, y \in H$, the cyclic subgroup of G generated by z, such that

(1) $z = x \Box y$

(2) the period of x is m, the period of y is n

(3) $x \Box y = y \Box x$

(4) this representation is unique.

PROOF: Let $u = z^n$, $v = z^m$. Then $u \Box v = v \Box u$, since u and v are powers of the same element. Also $u^m = e = v^n$, where e is the neutral element of G, and since z is of period mn, u must be of period m and v of period n.

Since $(m, n) = 1, \exists\, s, t \in Z \ni sm + tn = 1$ and $(s, n) = 1$, $(t, m) = 1$. Hence, $z = z^{sm+tn} = (z^n)^t \Box (z^m)^s = u^t \Box v^s$. By Problem 2.15, u^t is of period m, and v^s is of period n. Thus, if we take $x = u^t$, $y = v^s$, we have the first three statements of the conclusion established.

To prove uniqueness, let $z = x \Box y = x_1 \Box y_1$, where $x \Box y = y \Box x$, $x_1 \Box y_1 = y_1 \Box x_1$, x and x_1 are of period m, y and y_1 are of period n. Then, with s and t as before, we have $x^{tn} \Box y^{tn} = x_1^{tn} \Box y_1^{tn} \Rightarrow x^{tn} = x_1^{tn}$ (since y, y_1 are of period n) $\Rightarrow x^{1-sm} = x_1^{1-sm} \Rightarrow x \Box (x^m)^{-s} = x_1 \Box (x_1^m)^{-s} \Rightarrow x = x_1$. Then, since G is a group, $y = y_1$. ■

Problem 7.1 State and prove Theorem 7.1 with addition as the law of composition.

Problem 7.2 Apply Theorem 7.1 to $z = a^2$ in the cyclic group of order 24 generated by a.

Problem 7.3 Let $(G, \square)$ be a cyclic group of order mn with $(m, n) = 1$, $m > 1$, $n > 1$. Prove that there exist two proper subgroups H_1, H_2 of G such that every element of G can be expressed uniquely as a product of an element of H_1 and an element of H_2.

Definition 7.1 Let $(G, \square)$ be a group, let $a, b \in G$, and let H_1, H_2 be subgroups of G. Then

(1) a and b are *permutable* $\Leftrightarrow a \square b = b \square a$.

(2) a and H_1 are *permutable* $\Leftrightarrow a \square H_1 = H_1 \square a$.

(3) H_1 and H_2 are *permutable* $\Leftrightarrow$ every element of H_1 is permutable with H_2 and every element of H_2 is permutable with H_1.

Problem 7.4 Prove that a and a subgroup H_1 of a group $(G, \square)$ are permutable $\Leftrightarrow \forall h_1 \in H_1 \; \exists h_2 \in H_1 \ni a \square h_1 = h_2 \square a$.

Problem 7.5 Prove that a subgroup H of a group G is invariant if and only if every element of G is permutable with H.

Problem 7.6 Prove that if H is a subgroup of a group G, then every element of H is permutable with H.

Definition 7.2 A group $(G, \square)$ is the *direct product* (or *direct sum* if the law of composition is addition) of its subgroups, H_1, H_2, …, $H_n \Leftrightarrow$

(1) every element of H_i is permutable with every element of H_j for $i \neq j$, $i, j = 1, 2, \ldots, n$,

(2) $x \in G \Rightarrow \exists$ unique $u_i \in H_i \ni x = \square_{i=1}^{n} u_i$. The element u_i in this representation is called the *component* of x in H_i.

If the law of composition in G is addition and if G is the direct sum of the subgroups H, K, we write $G = H \oplus K$, with obvious generalization to more than two subgroups.

Problem 7.7 Show that the cyclic group of order 12 is the direct product of cyclic subgroups of orders 3 and 4. Find the group product of a cyclic group of order 3 and a cyclic group of order 4 and show that it is isomorphic to the preceding group.

Problem 7.8 Show that the group product of two cyclic groups of relatively prime orders is a cyclic group of order the product of the orders of the original groups and show that it is the direct product of two subgroups isomorphic to the original groups.

Problem 7.9. Show that any cyclic group of order mn, where $(m, n) = 1, m > 1, n > 1$, is the direct product of two cyclic subgroups of orders m, n.

Problem 7.10. Show that the cyclic group of order 9 is not the direct product of two of its subgroups. Generalize.

Problem 7.11. Show that the 4-group (any group isomorphic to the group of Problem 10.1 of Chapter 2) is the direct sum of two cyclic subgroups of order 2.

Problem 7.12. Show that the direct sum of two abelian groups is abelian.

Problem 7.13. Prove: $G = H \oplus K, H, K$ of orders h, k, respectively $\Rightarrow G$ is of order hk. Generalize.

Problem 7.14. Find all abelian groups of order 8.

Problem 7.15. Prove: $G = H \oplus K \Rightarrow G/H$ is isomorphic to K, G/K is isomorphic to H.

Theorem 7.2. The group G is the direct product of its subgroups $H_1, H_2, \ldots, H_n \Leftrightarrow$

(1) the subgroups $H_1, H_2, \ldots, H_n$ are invariant subgroups of G

(2) G is generated by the subgroups $H_1, H_2, \ldots, H_n$ (cf. Definition 2.1.)

(3) the common part of each H_i with the subgroup H_i', generated by all the H_j, $i \neq j$, is $\{e\}$, the subgroups consisting of the neutral element of G.

Proof: (In this proof, numbers prefixed by D refer to conditions of Definition 7.2 and numbers prefixed by T refer to conditions of Theorem 7.2.)

The theorem is trivially true if $n = 1$, so we suppose that $n \geqslant 2$. Consider the implication $\Rightarrow$. First, we note that D2 $\Rightarrow$ T2. To show that T3 holds, let c belong to the common part of H_1 and H_1'. Then $c = h_2 \square \cdots \square h_n$, where $h_i \in H_i, i = 2, 3, \ldots, n$, and also $c = h_1 \in H_1$. Then we have two distinct representations of c, contrary to D2. The same is true for any i. Therefore, condition T3 holds.

To prove T1, let $k_i \in H_i$ and $g \in G$. Then $g = h_1 \square h_2 \square \cdots \square h_i \square \cdots \square h_n$ by D2, so $g^{-1} \square k_i \square g = h_n^{-1} \square h_{n-1}^{-1} \square \cdots \square h_i^{-1} \square \cdots \square h_1^{-1} \square k_i \square h_1 \square \cdots \square h_{n-1} \square h_n = h_i^{-1} \square k_i \square h_i$ by condition D1) and this last element belongs to H_i. Therefore, H_i is invariant in G.

Consider now the implication $\Leftarrow$. To prove D1, let $h_i \in H_i$ and $h_j \in H_j, i \neq j$. Then $h_i^{-1} \square h_j^{-1} \square h_i \in H_j$, since H_j is invariant, and similarly, $h_j^{-1} \Box h_i \Box h_j \in H_i$. Hence, $(h_i^{-1} \Box h_j^{-1} \Box h_i) \Box h_j \in H_j$ since each of the two indicated factors $\in H_j$ and H_j is a group, and similarly, $h_i^{-1} \Box (h_j^{-1} \Box h_i \Box h_j) \in H_i$. Now by T3, $H_i \cap H_j = \{e\}$. Therefore $h_i^{-1} \Box h_j^{-1} \Box h_i \Box h_j = e$, and so by multiplying on the left by h_i, and then by h_j, we get successively, $h_j^{-1} \Box h_i \Box h_j = h_i$, $h_i \Box h_j = h_j \Box h_i$. Therefore, condition D1 holds.

To prove D2, we observe that T2 gives us at least one representation of each x in G in the desired form (using D1 is necessary). Let us suppose that we have two such, say, $x = u_1 \Box u_2 \Box \cdots \Box u_n = v_1 \Box v_2 \Box \cdots \Box v_n$, where at least one $u_i \neq v_i$, say $u_1 \neq v_1$ (since the u's are permutable and so are the v's, it makes no difference which we suppose are unequal). $u_1, v_1 \in H_1$. Then we have $v_1^{-1} \Box u_1 = (v_2 \Box \cdots \Box v_n) \Box (u_n^{-1} \Box \cdots \Box u_2^{-1}) = (v_2 \Box u_2^{-1}) \Box \cdots \Box (v_n \Box u_n^{-1})$, by permutability, and here the element on the left $\in H_1$ and the one on the right $\in H_1$. This is impossible by T3 unless each element is equal to e. Then $u_1 = v_1$, etc. Therefore D2 holds. ■

THEOREM 7.3. In Theorem 7.2, condition (3) may be replaced by

(4) the common part of H_i, $i = 2, 3, \ldots, n$, with the subgroup generated by $H_1, \ldots, H_{i-1}$ is $\{e\}$.

PROBLEM 7.16. Prove Theorem 7.3.

8 PRODUCTS OF SUBGROUPS OF GROUPS

We have been considering the direct products of two or more subgroups of a group and among other conditions the subgroups had no elements in common other than the neutral element and each element of one subgroup was permutable with every element of every other subgroup. Under these conditions, the product was a subgroup and in the case of finite groups, its order was the product of the orders of the subgroups. We shall now consider what happens when we drop these two conditions and consider merely the product of two subgroups, H and K, in accordance with Definition 3.1. Theorem 8.1 gives us the result about the number of elements and Theorem 8.2 gives the condition under which the product is a group.

THEOREM 8.1. Let A and B be finite subgroups of order a, b, respectively, of a group $\langle G, \Box \rangle$ and $C = A \cap B$ be of order c. Then the product $A \Box B$ has exactly ab/c elements.

PROOF. By Theorem 3.3, $B = (C \Box b_1) \cup (C \Box b_2) \cup \cdots \cup (C \Box b_n)$, where $b_i \notin C$ for $i > 1$, and $C \Box b_i \neq C \Box b_j$, if $i \neq j$,

$n = b/c$. Thus $A \square B = [(A \square C) \square b_1] \cup \cdots \cup [(A \square C) \square b_n]$. Now by Problem 3.10, $A \square C = A$, since $C \subset A$. Hence we have $A \square B = (A \square b_1) \cup (A \square b_2) \cup \cdots \cup (A \square b_n)$. Further, $(A \square b_i) \cap (A \square b_j) = \varnothing$, if $i \neq j$, since if $x \in (A \square b_i) \cap (A \square b_j), i \neq j$, we should have $x = a_1 \square b_i = a_2 \square b_j$, where $a_1, a_2 \in A$. Then $a_2^{-1} \square a_1 = b_j \square b_i^{-1}$ would belong both to A and to B and so to C, but this would make $C \square b_i = C \square b_j$, contrary to the representation of B given at the beginning. Hence, the sets $A \square b_i$ are disjoint, there are $n = b/c$ of them and there are a elements in each one. Hence, the number of elements in $A \square B$ is $a \cdot b/c$. ■

THEOREM 8.2. Let A and B be subgroups of a finite group $\langle G, \square \rangle$. Then $D = A \square B$ is a subgroup of $G \Leftrightarrow A \square B = B \square A$.

PROOF: Consider the implication $\Rightarrow$. Let $D = A \square B$ be a subgroup of G, and let $a \in A$, $b \in B$. Then $a^{-1} \in A$, $b^{-1} \in B$ and so $a^{-1} \square b^{-1} \in A \square B$. Since D is a group, $(a^{-1} \square b^{-1})^{-1} = b \square a \in D$. Thus, $\forall a \in A$, $\forall b \in B$, $b \square a \in A \square B$. Therefore, $B \square A \subset A \square B$. However, since the number of distinct elements in $A \square B$ and $B \square A$ is finite and the same (obviously from Theorem 8.1), $A \square B = B \square A$.

Now consider the implication $\Leftarrow$. Let $A \square B = B \square A = D$. Then $D^2 = (A \square B) \square (A \square B) = A \square (B \square A) \square B = A \square (A \square B) \square B = A^2 \square B^2 = A \square B$, by Problem 3.8. Hence also by Problem 3.8, D is a subgroup of G. ■

We shall now consider a special case of the product of two subgroups. Let H be a subgroup of order h of $\langle G, \square \rangle$, and K a cyclic subgroup of G generated by the element a of period n, and let a^m be the lowest positive power of a which is in H. We shall first prove that $m|n$. If we let $d = (m, n)$, we have by Theorem 17.3 of Chapter 2, $sm + tn = d$, where $s, t \in Z$. Now $a^d = a^{sm+tn} = a^{sm} \square (a^n)^t = a^{sm}$ and so $a^d \in H$. Hence, d cannot be less than m and so $d = (m, n) = m$. Therefore, $m|n$. ■

Now since $a^m \in H$, its period n/m must divide h. We have now proved

THEOREM 8.3. H is a subgroup of order h of a group G, $a \in G$, a has period n, $a^m \in H$ and $a^k \notin H$ for $0 < k < m \Rightarrow m|n$ and $n/m|h$.

THEOREM 8.4. Let H_1 and H_2 be two subgroups of a group G with the properties:

(1) each element of H_1 is permutable with H_2 and each element of H_2 is permutable with H_1.

(2) $H_1 \cap H_2 = \{e\}$
Then each element of H_1 is permutable with each element of H_2

Corollary 8 1 If H_1 and H_2 are invariant subgroups of a group G and if $H_1 \cap H_2 = \{e\}$, where e is the neutral element of G, then $H_1 \square H_2$ is the direct product of H_1 and H_2

Theorem 8 5 If H_1, H_2 are invariant subgroups of a group G, then the group generated by H_1 and H_2 is $H_1 \square H_2$

Problem 8 1 Prove Theorem 8 4 (Hint let $a \in H_1, b \in H_2$ and consider $a^{-1}b^{-1}ab$ as in the proof of Theorem 7 2)

Problem 8 2 Prove Corollary 8 1

Problem 8 3 Prove Theorem 8 5 generalize, and prove your generalization

9 FREE GROUPS

Thus far the methods we have used for finding actual specific groups have been those of considering a set of 1–1 mappings of a set E, subsets of Z and of forming product groups or quotient groups from groups already known We shall now consider another method Certain aspects of this method may remind the reader of the methods used in the proofs of Theorems 1 3 and 1 5 but it should be borne in mind that in those proofs we were operating in a group or a semigroup from the very beginning Here we are not

Definition 9 1 Let A be a set and $E = A \times \{1, -1\}$ We shall write the element of E as a^{ϵ} where $a \in A$ and $\epsilon \in \{1, -1\}$ A finite sequence of elements of E is a *word* Two elements a_i, a_j of a word are called *adjacent* if and only if either $i = j + 1$ or $j = i + 1$ We shall write adjacent elements in a word next to each other without commas etc Thus a word may be written in the form $w = x_{c_1}^{\alpha_1} x_{c_2}^{\alpha_2} \cdots x_{c_n}^{\alpha_n}$ where $\alpha_i = \pm 1$ $i = 1, 2, \ldots, n$ The word w is a *reduced word* if and only if no symbol x_i^{+1} is adjacent to x_i^{-1} In a reduced word w, the number of elements actually present is the *length of the word* and is denoted by $L(w)$ Further the null set is called the *empty word*, and is denoted by w_0 and $L(w_0) = 0$ Lastly, the *product* of the words $w_1 = x_{c_1}^{\alpha_1} x_{c_2}^{\alpha_2} \cdots x_{c_n}^{\alpha_n}$ and $w_2 = x_{d_1}^{\beta_1} x_{d_2}^{\beta_2} \cdots x_{d_m}^{\beta_m}$ is $w_1 w_2 = x_{e_1}^{\gamma_1} x_{e_2}^{\gamma_2} \cdots x_{e_{n+m}}^{\gamma_{n+m}}$ where $e_i = c_i$, $\gamma_i = \alpha_i$, for $i = 1, 2, \ldots, n$, and $e_i = d_{i-n}$, $\gamma_i = \beta_{i-n}$ for $i = n + 1, n + 2, \ldots, n + m$

The set M of all words formed from E with product defined as above, is easily seen to be a semigroup with a neutral element, since it is easy to prove that this law of composition is associative. M, however, is not a group since no element other than the neutral element has an inverse. We shall now proceed, as we have often done before, to introduce an equivalence relation in M, and then prove that the quotient set is a group.

Definition 9.2. Two words, w_1, w_2 are *adjacent* $\Leftrightarrow$ either $w_1 = ux_c^{\delta}x_c^{-\delta}v$ and $w_2 = uv$, where u and v are words, or $w_1 = uv$ and $w_2 = ux_c^{\delta}x_c^{-\delta}v$, where $\delta = \pm 1$. Two words are *equivalent*, written $w_1 \equiv w_2 \Leftrightarrow \exists$ a finite set of words $u_1, u_2, \ldots, u_m \ni u_i$ and u_{i+1} are adjacent, $i = 1, 2, \ldots, m-1$, $w_1 = u_1$ and $w_2 = u_m$.

We leave to the reader the task of showing that $\equiv$ is an equivalence relation.

Problem 9.1. Prove that the product of words is associative.

Problem 9.2. Prove that $\equiv$ is an equivalence relation.

Problem 9.3. Find a reduced word equivalent to w_1w_2 where $w_1 = x_3^{+1}x_7^{-1}x_1^{+1}x_4^{+1}x_4^{+1}$, $w_2 = x_4^{-1}x_5^{+1}x_5^{-1}x_{173}^{+1}x_5^{-1}x_3^{-1}x_7^{-1}$. Do the same for w_2w_1. In both cases, find the intermediate words.

Problem 9.4. Proceed as in Problem 9.3 for

$$w_1 = x_1^{+1}x_1^{+1}x_1^{+1}x_2^{-1}x_2^{-1}x_1^{+1}, \quad w_2 = x_1^{-1}x_2^{+1}x_2^{+1}x_1^{-1}.$$

Problem 9.5. Find equivalence classes which are the inverses of the classes containing w_1 and w_2 of Problem 9.4.

Theorem 9.1. The equivalence relation of Definition 9.2 is compatible with the product as defined in Definition 9.1.

Proof: Let $f \equiv h$ and $g \equiv k$, and let $f = u_1, u_2, \ldots, u_n = h$ be a set of words such that u_i, u_{i+1} are adjacent for $i = 1, 2, \ldots, n-1$, $g = v_1, v_2, \ldots, v_m = k$ be a set of words such that v_j, v_{j+1} are adjacent for $j = 1, 2, \ldots, m = 1$. Then u_ig, $u_{i+1}g$ are adjacent for $i = 1, 2, \ldots, n-1$, and hv_j, hv_{j+1} are adjacent for $j = 1, 2, \ldots, m-1$. Hence, since $u_ng = hg = hv$, we have the set of words $fg, u_2g, \ldots, u_{n-1}g, hg, hv_2, \ldots, hv_{m-1}, hk$ in which each consecutive pair is a pair of adjacent words. Therefore, $fg \equiv hk$. ∎

Theorem 9.2. The quotient set of M of Definition 9.1 with respect to the equivalence relation of Definition 9.2 is a group F called the *free group generated by the set* A.

Proof: Let F be the quotient set. Since M is a semigroup, by Theorem 9.1 above and Theorems 12.1 and 12.2 of Chapter 2, F is a semigroup. Since M has a neutral element w_0, the equivalence class containing w is a neutral element for F. If $w = x_{c_1}^{\alpha_1} x_{c_2}^{\alpha_2} \cdots x_{c_n}^{\alpha_n}$ then the equivalence class containing $x_{c_n}^{-\alpha_n} x_{c_{n-1}}^{-\alpha_{n-1}} \cdots x_{c_1}^{-\alpha_1}$ is an inverse for the equivalence class containing w. Therefore F is a group. ■

DEFINITION 9.3 The cardinal number of the elements in the set A is called the *rank* of the free group F generated by A.

PROBLEM 9.6 Prove that a free group of rank 1 is cyclic and is isomorphic to the additive group of Z.

THEOREM 9.3 In a free group F no element except the neutral element has finite period.

PROOF Let $w = x_{c_1}^{\alpha_1} x_{c_2}^{\alpha_2} \cdots x_{c_n}^{\alpha_n}$ be a word not equivalent to the empty word. Then it may be that $x_{c_1}^{\alpha_1}$ and $x_{c_n}^{\alpha_n}$, $x_{c_2}^{\alpha_2}$ and $x_{c_{n-1}}^{\alpha_{n-1}}$, $\ldots$, $x_{c_k}^{\alpha_k}$ and $x_{c_{n-k+1}}^{\alpha_{n-k+1}}$ are pairs of inverses, but by the hypothesis made on w, $\exists k \ni x_{c_{k+1}}^{\alpha_{k+1}}$ and $x_{c_{n-k}}^{\alpha_{n-k}}$ are not inverses of each other. Then we let $v = x_{c_{k+1}}^{\alpha_{k+1}} \cdots x_{c_{n-k}}^{\alpha_{n-k}}$ and we have $\forall s \in Z^*$ $w^s = x_{c_1}^{\alpha_1} \cdots x_{c_k}^{\alpha_k} v^s x_{c_{n-k+1}}^{\alpha_{n-k+1}} \cdots x_{c_n}^{\alpha_n}$ which is a reduced word $\neq$. It is clear from Definition 9.2 that two words are equivalent if and only if we can go from one to the other by inserting or suppressing a finite number of $x_c^{\beta} x_c^{-\beta}$. So if two words are equivalent at least one of them must have one or more (unsuppressed) $x_c^{\beta} x_c^{-\beta}$. Two reduced words do not. Thus two distinct reduced words must be inequivalent. Hence w^s is not equivalent to the empty word. ■

THEOREM 9.4 Every group is isomorphic to a quotient group of a free group.

PROOF Let G be a group and M a set of generators of G (there always exists a set of generators for any group, if necessary take all the elements of G as M). Let W be any set of elements such that there exists a 1-1 mapping α of W onto M and let F be the free group generated by W. If we then for $x_c \in F$ denote $x_c\alpha$ by a_c, we have a mapping of F onto G such that $(x_{c_1}^{\beta_1} \cdots x_{c_n}^{\beta_n})\alpha = a_{c_1}^{\beta_1} \cdots a_{c_n}^{\beta_n}$ which is obviously a homomorphism of F onto G. Hence by Theorem 4.1 G is isomorphic to F/H, where H is the normal subgroup of F consisting of all equivalence classes containing all words $x_{c_1}^{\beta_1} \cdots x_{c_n}^{\beta_n}$ whose images $a_{c_1}^{\beta_1} \cdots a_{c_n}^{\beta_n}$ are all equal to the neutral element of G. ■

DEFINITION 9.4 Let $x_{c_1}^{\beta_1} \cdots x_{c_n}^{\beta_n}$ be any word in H of the above proof. Then the equation $a_{c_1}^{\beta_1} \cdots a_{c_n}^{\beta_n} = 1$ implied by the isomorphism α is a relation between elements of M. Let K be a set of elements such that the normal subgroup H of F of the above proof is generated by K, then the set of relations in G corresponding to the elements of K is called a *set of defining relations of* G.

EXAMPLE 9.1. Let G be the cyclic group of order n. Here we may take $M = \{a\}$, where a is a generator of G. We may take $W = \{s\}$. Then H will consist of the set $\{s^{kn}\}$, $\forall\, k \in Z$. Since s^n is a generator of H, a set of defining relations of G will consist of the single equation $a^n = 1$.

PROBLEM 9.7. Let G be the abelian group of order 9 which is the direct product of two of its cyclic subgroups of order 3. Find a quotient group of a free group isomorphic to G.

Using Theorem 9.4 we can start with a group and find a set of defining relations. However, we can also proceed in the opposite direction as well. That is, we may start with a set A of symbols and an arbitrary set of relations equating certain words formed from these symbols to 1, and there will always be a group for which these relations form a set of defining relations. For, we may take the free group generated by A and the normal subgroup generated by the nonempty sides of the given equations and the quotient group will be a group with the desired defining relations.

EXAMPLE 9.2. *Cyclic group of order n, C_n.* Here we need only one defining relation: $a^n = 1$ where a is a generator of C_n. If any lower power of a were 1, this would imply an additional relation.

EXAMPLE 9.3. *Dihedral group of order $2n$, D_{2n}.* (See Section 5 above.)

EXAMPLE 9.4. *Quaternion group of order $4n$, Q_{4n}.* (See Section 5 above.)

PROBLEM 9.8. Give defining relations for the group of Problem 9.7.

PROBLEM 9.9. Discuss the general groups D_{2n} and Q_{4n}.

THEOREM 9.5. If a group G is given by a set of defining relations and a group G' is given by a set of defining relations, which includes all the defining relations of G, then G' is isomorphic to a quotient group of G.

PROBLEM 9.10. Prove Theorem 9.5. (Hint: represent G, G' as quotient groups of the same free group.)

10 SYLOW THEOREMS

The converse of Lagrange s Theorem holds for cyclic groups, but not for all groups We shall, in the next section, give an example of a group of order 12 which does not have a subgroup of order 6, although $6|12$ In the present section we shall consider a theorem which is a partial converse of Lagrange's Theorem

DEFINITION 10 1 Let G be a finite group of order n and let $p \in Z^*$ where p is a prime Further, let p^m be the highest power of p (with positive exponent) which divides n Then a subgroup H of G is a *Sylow subgroup* $\Leftrightarrow$ the order of H is p^m

THEOREM 10 1 Let G be a finite group of order n and p be a positive rational prime dividing n Then G has at least one Sylow subgroup of order p^m

PROOF If $n = p^m$, the theorem is obviously true so we shall suppose that $n \neq p^m$ The theorem is obviously true if $n = 2$, and we shall proceed by induction by supposing that it is true for all orders less than n

(1) The central of G consists of the neutral element alone Then by Problem 6 1, the elements of G fall into disjoint sets of conjugate elements Let h_1 h_2, h_r be the numbers of elements in these sets In the case we are considering, one of the h_i say h_1, is 1 (this is the number of elements in the set containing the neutral element), and all the other h_i are greater than 1 We have then $n = 1 + h_2 + h_3$ $+ h_r$ Since $p|n$, and $p \nmid 1$ there must be at least one h_i, $i > 1$, say h_j, $\ni p \nmid h_j$ Now by Theorem 6 1 n/h_j is the order of a subgroup of G, namely the normalizer N of one of the elements of the complete set of conjugate elements whose number is h_j Thus $p^m|(n/h_j)$ and so by induction hypothesis N has a subgroup of order p^n and this subgroup is, of course, a subgroup of G

(2) The central of G has elements in addition to the neutral element Let s be one such element and we may suppose that its period is a prime for if s is of period rk, where r is a prime, then s^k is of period r, and s^k belongs to the central

(2a) s is of period p Let S be the cyclic subgroup of G generated by s Then G/S is a group of order n/p and $p^{m-1}|(n/p)$ and so G/S has a subgroup S' of order p^{m-1} Then by Theorem 4 4 G has a subgroup H corresponding to S , and the order of H must be p^m

(2b) s is of period $q \neq p$ Let S be as before Then the order of G/S is divisible by p^m and if it is not p^m, then, as before, G has a proper subgroup whose order is divisible by p^m and so by induction hypothesis, this subgroup, and G also, has a subgroup of order p^m.

If the order of G/S is p^m, then G is of order $p^m q$. Since $s \in$ the central, C, of G, every element of $S \in C$. Thus, for each element of G, the normalizer contains S. Hence, the order of each normalizer is divisible by q, and so, by Theorem 6.1, no h_i (of case 1) is divisible by q. Hence, in the notation of case 1, $p^m q = 1 + h_2 + \cdots + h_4$, where none of the h_i is divisible by q, and since there are at least q ones, there must be more than q ones. Thus there must be an element $t \in C \ni t \notin S$. The period of t must be divisible by p, and not by q, since G cannot contain a subgroup of order q^2. (There would be a subgroup of this order, since $t, s \in C$, and we may suppose, as before, that the period of t is p.) Let T be the cyclic subgroup of G, generated by t. Then G/T is of order $p^{m-1}q$ and so it contains a subgroup of order p^{m-1}. Hence, G has a subgroup of order p^m. ■

Corollary 10.1. (Cauchy's Theorem.) If a positive rational prime p divides the order of a finite group G, then G has elements of period p.

Corollary 10.2. If p^k divides the order of a finite group G, where p is a positive rational prime, then G has a subgroup of order p^k.

Problem 10.1. Prove Corollary 10.1.

Problem 10.2. Prove Corollary 10.2. (Hint: show by using the relation $n = 1 + h_2 + \cdots h_r$ of the proof of Theorem 10.1, that a group of order p^m has a central of order at least p; then proceed by induction.)

Example 10.1. We shall determine all groups of order p^2, where p is a positive rational prime. Let G be such a group. If G has an element of period p^2, then G is cyclic. If not, then its $p^2 - 1$ elements, other than the neutral element, must all be of period p. A subgroup of order p contains $p - 1$ elements of period p and none of these can be in any other subgroup of order p. Therefore, there must be $(p^2 - 1)/(p - 1) = p + 1$ subgroups of order p. By Corollary 6.2, the number of subgroups in a complete set of conjugate subgroups must divide the order of the group, namely, p^2, and so at least one of these $p + 1$ subgroups must be invariant. Let a be a generator of this subgroup G. and let b be any element of period $p \ni b \in H$. Then $b^{-1}Hb = H$. Hence, $b^{-1}ab = a^k$, for some $k \in Z^*$, $0 < k < p$. Hence, $b^{-1}ab^i = a^{k^i}$ and finally, $b^{-p}ab^p = a^{k^p} = a \Longrightarrow k^p \equiv 1 \mod p$. But, $k^{p-1} \equiv 1 \mod p$ and so $k \equiv 1 \mod p$. But, $0 < k < p$ and $k \equiv 1 \mod p$

$\Rightarrow k = 1$ Therefore $ab = ba$ and so G is an abelian group which is either cyclic or the direct product of two cyclic subgroups of order p

PROBLEM 10 3 By using the first Sylow Theorem and the type of reasoning used in the above example show that if a group has *order pq where p and q are distinct positive rational primes with* $p < q$ then either G is cyclic and this is the only possible case if $q \neq 1 \bmod p$ or if $q \equiv 1 \bmod p$ G may be non abelian (Hint in this latter case if a b are elements of periods p q respectively then the defining relations will be $a^p = b^q = 1$ $a^{-1}ba = b^{\beta}$ where β is a root of $\beta \equiv 1 \bmod q$ $\beta \neq 1$)

THEOREM 10 2 Let G be a finite group of order n and p be a positive rational prime such that p^m is the highest power of p dividing n Then the Sylow subgroups of order p^m form a complete set of conjugate subgroups and the number of them is congruent to 1 mod p

PROOF (1) We shall first prove that if H is a Sylow subgroup of G of order p^m then the only elements of G which are permutable with H and have periods which are powers of p are the elements of H

Let s be an element of period p^k permutable with H and let K be the subgroup generated by s Then $HK = KH$ and so by Theorem 8 2 HK is a subgroup of G If the lowest positive power of s which is in H is s^{p^h} (cf first conclusion of Theorem 8 3) then $H \cap K$ is of order p^{k-h} (since the powers of s which are in H will be $(s^{p^h})^j$ $j = 1$ 2 p^{k-h}) and so by Theorem 8 1 the order of HK is $p^m p^k / p^{k-h} = p^{m+h} > p^m$ which is impossible since H is a Sylow subgroup Therefore $s \in H$

(2) We shall next prove that if H and H_1 are two subgroups of order p^m and if $K_1 = H \cap H_1$ is of order p^{β} then the elements of H transform H_1 into exactly $p^{m-\beta}$ conjugate subgroups

By the result just established the only elements of H which transform H_1 into itself will be the elements of K_1 There are $p^{m-\beta}$ cosets of H with respect to K_1 and the elements of each coset obviously transform H_1 into the same conjugate subgroup while the elements of two different cosets give different subgroups conjugate to H_1 (For if $h_1^{-1} H_1 h_1 = h_2^{-1} H_1 h_2$ then $H_1 = h_1 h_2^{-1} H_1 h_2 h_1^{-1} = (h_2 h_1^{-1})^{-1} H_1 (h_2 h_1^{-1})$ and so $h_2 h_1^{-1} \in K_1$ Thus h_1 h_2 are members of the same right coset

(3) If H H_1 are Sylow subgroups of order p^m and H_1 is conjugate to H then by (2) there are at least $1 + p^{m-\beta}$ distinct subgroups conjugate to H namely H itself and the $p^{m-\beta}$ subgroups conjugate to H_1 obtained in (2)

(4) By induction it follows easily that the total number of subgroups conjugate to H is of the form $1 + p^{m-\beta_1} = p^{m-\beta_2} + \cdots + p^{m-\beta_n}$ and so is conjugate to 1 mod p.

(5) If there exists another Sylow subgroup L, and if L is not conjugate to H, then by continued application of (2), we find that the number of Sylow subgroups in the complete set containing L is the sum of positive powers of p and so is congruent to 0 mod p. But the above reasoning now applied to L instead of H shows that the number is congruent to 1 mod p. Therefore, the Sylow subgroups of order p^m form a complete set of conjugate subgroups. ■

Corollary 10.3. There is only one Sylow subgroup H of order p^m of $G \Leftrightarrow H$ is an invariant Sylow subgroup of G.

Definition 10.2. A group G is *simple* if and only if no proper subgroup of G is invariant.

As examples of application of the second Sylow Theorem:

Example 10.2. We shall show that no group of order 30 is simple. Such a group G would have $5 + 1$ Sylow subgroups of order 5 and so $6 \cdot 4$ elements of period 5. Also, there would be at least $1 + 3 = 4$ Sylow subgroups of order 3 containing $4 \cdot 2 = 8$ elements of period 3. We have now, including the neutral element, at least $24 + 8 + 1$ distinct elements and we have not yet considered the Sylow subgroups of order 2. We have thus too many elements and so G cannot be simple.

Example 10.3. A group G of order pq, where p and q are distinct primes such that $p \not\equiv 1$ mod q and $q \not\equiv 1$ mod p is abelian. For, the number of Sylow subgroups of order p must divide q by Theorem 6.2 and also must be $\equiv 1$ mod p by Theorem 10.2. Therefore, by the condition $q \not\equiv 1$ mod p, such a Sylow subgroup must be invariant. Similarly, a Sylow subgroup of order q must be invariant. Therefore, by Theorem 8.2, G is the product of these subgroups and since their common part (by an obvious consideration of periods) is the neutral element, by Corollary 8.1, G is the direct product of these two cyclic subgroups of distinct prime orders, and so G is cyclic and also abelian.

Problem 10.4. Find all Sylow subgroups of S_3 and verify Theoiem 10.2.

Problem 10.5. Prove that no group of order 56 is simple.

Problem 10.6. Prove that G is abelian if G is a group of order p^2q, where p and q are positive primes such that $q < p$ and $q \nmid p^2 - 1$.

PROBLEM 10.7 Prove that if every Sylow subgroup of a group G is invariant, then G is the direct product of its Sylow subgroups.

11 PERMUTATIONS AND PERMUTATION GROUPS

DEFINITION 11.1 A 1–1 mapping of a set E onto itself is called a *permutation* of E. The set of all permutations of E is called the *symmetric group* of the set E and is denoted by S_E. If E is a finite set of n objects S_E it is often called the *symmetric group of degree n* and is denoted by S_n. In this case each element is said to be of *degree n*.

PROBLEM 11.1 Find S_3.

PROBLEM 11.2 Show that S_n is of order $n!$

DEFINITION 11.2 A 1–1 mapping α of a group $(G, \square)$ onto a group $(H, \bigcirc)$ is an *anti isomorphism* of G onto $H \Leftrightarrow \forall a, b \in G$ $(a \square b)\alpha = (b\alpha) \bigcirc (a\alpha)$. If $G = H$, the mapping is called an *anti automorphism*.

DEFINITION 11.3 Let E be a set which is closed with respect to an internal law of composition $\square$. A *right (left) translation of E* $\delta_a(\gamma_a)$ determined by $a \in L$ is the mapping of E into itself defined by $x\delta_a = x \square a$ $(x\gamma_a = a \square x)$ $\forall x \in E$.

THEOREM 11.1 The set $T_R\,(T_L)$ of all right (left) translations of a group G forms a subgroup of S_G and $T_R\,(T_L)$ is isomorphic (anti isomorphic) to G.

PROOF. δ_a is a 1–1 mapping since if $x \square a = y \square a$ then because G is a group $x = y$.

δ_a is an onto mapping since if $u \in G$ $\exists y \in G \ni y \square a = u$. Thus $y\delta_a = u$.

T_R is closed since $x(\delta_a\delta_b) = (x\delta_a)\delta_b = (x \square a)\delta_b = (x \square a) \square b = x \square (a \square b) = \delta_{a \square b}$.

The identity mapping is δ_e where e is the neutral element of G, and obviously δ_e is the neutral element of T_R.

Each δ_a has an inverse $\delta_{a^{-1}}$ since $(x\delta_a)\delta_{a^{-1}} = (x \square a)\delta_{a^{-1}} = (x \square a) \square a^{-1} = x \square (a \square a^{-1}) = x \square e = x\delta_e \Rightarrow \delta_a\delta_{a^{-1}} = \delta_e$. Similarly $\delta_{a^{-1}}\delta_a = \delta_e$. Therefore since the associative law obviously holds in G, T_R is a subgroup of S_G. Similarly T_L is a subgroup of S_G.

Next we prove that the mapping $a \to \delta_a$ $\forall a \in G$ is an isomorphism of G onto T_R. That it is a 1–1 onto mapping is obvious. That $a \square b \to \delta_a\delta_b$ follows from the third sentence of the proof. Therefore it is an isomorphism.

We leave the proof that $a \to \gamma_a$ is an anti-isomorphism of G onto T_l to the reader. ■

Corollary 11.1. (Cayley.) Every finite group G of order n is isomorphic to a permutation group of order n and degree n.

Corollary 11.2 Every group G is isomorphic to a group of left translations.

Problem 11.3. Complete the proof of Theorem 11.1.

Problem 11.4. Prove Corollary 11.2. (Hint: use the mapping $a \to \gamma_{a^{-1}}$.)

Problem 11.5. Find T_R and T_L for S_3.

Problem 11.6. Find for S_3 the group of Corollary 11.2.

Theorem 11.2. Every element of T_R is permutable with every element of T_L. Further, if β is a mapping of G into G, permutable with every $\gamma_a(\delta_a)$, then $\beta \in T_R(T_l)$.

Proof: $x(\gamma_a\delta_b) = (x\gamma_a)\delta_b = (a \square x)\delta_b = (a \square x) \square b = a \square (x \square b) = a \square (x\delta_b) = (x\delta_b)\gamma_a = x(\delta_b\gamma_a)$, $\forall\, x \in G$. Therefore, $\gamma_a\delta_b = \delta_b\gamma_a$.

Let β be any mapping of G into $G \ni \beta\gamma_x = \gamma_x\beta, \forall\, x \in G$; then $x\beta = (x \square e)\beta = (e\gamma_x)\beta = e(\gamma_x\beta) = e(\beta\gamma_x) = (e\beta)\gamma_x = x \square (e\beta) = x \square b$ where $b = e\beta$, Therefore, $\beta = \delta_b$. We leave the other case to the reader. ■

Problem 11.7. Finish the proof of Theorem 11.2.

Definition 11.4. A permutation P on the n objects $a_1, a_2, \ldots, a_n$ is a *cycle* (also called a *cyclic permutation* or a *circular permutation*) if and only if there exists a subset $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ of the a's such that under P, $a_{i_j} \to a_{i_{j+1}}$ for $j = 1, 2, \ldots, k-1$, $a_{i_k} \to a_{i_1}$, while $a_w \to a_w$ for $w \neq i_j, j = 1, 2, \ldots, k$.

Two or more cycles are *disjoint* if and only if the subsets involved are disjoint.

Theorem 11.3. A cycle, $P \in S_n$, which leaves $n-k$ of the $a_1, a_2, \ldots, a_n$ unchanged is of period k.

Proof: If $j > 0$, then under $P^j, a_{i_p} \to a_{i_q}$, where $q \equiv p + j \bmod k$ and $1 \leqslant q \leqslant j$. If $P^j = e$, then $p = q$, $\forall\, p$, and so the smallest j for which this is true is $j = k$. Therefore, P is of period k. ■

Theorem 11.4. A permutation $P \neq 1, P \in S_n$, can be expressed as a product of disjoint cycles uniquely except for the order of the factors.

Problem 11 8 Prove Theorem 11 4

Problem 11 9 Express $\begin{pmatrix} a_1a_2a\ a_4a_5a_6 \\ a_2a_4a_3a_1a_6a_3 \end{pmatrix}$ in the form of Theorem 11 4

Problem 11 10 Do the same as Problem 11 9 for $\begin{pmatrix} abcde \\ dbeac \end{pmatrix}$

Problem 11 11 Prove that the period of a permutation is the l c m of the periods of the disjoint cycles of which it is the product

A matter of notation Since in a cyclic permutation all objects not in the subset given in Definitions 11 4 are mapped each onto itself they may be omitted and the cyclic permutation of Definition 11 4 may be written as $\begin{pmatrix} a\ a_2 & & a_k \\ a_{i_1}a_{i_2} & & a \end{pmatrix}$ and repetition of symbols may be avoided by writing this on one line as $(a\ a_2 \qquad a_k)$ with the under standings that

(1) each element except the last is mapped onto the one which succeeds it

(2) the last element is mapped onto the first (of course any ele ment not listed is mapped onto itself) If it be desired to indicate all the n objects involved this last may be written as $(a \qquad a_k)(a_{k+1})$ (a_{i_n}) where each of the a_j, $j > k$ is mapped onto itself

Also we may omit the letter a and write the permutation merely in terms of the subscripts thus $(a\ a_2 \qquad a_k) - (i\ i \qquad i_k)$

Problem 11 12 Write as a product of disjoint cycles in single line form $\begin{pmatrix} 123456789 \\ 312465987 \end{pmatrix}$

Problem 11 13 Repeat Problem 11 12 for (123)(256)(789)(78)(12)

Definition 11 5 A cycle of degree n in which each of exactly $n-2$ objects is mapped onto itself is called a *transposition*

Theorem 11 5 A permutation can be expressed as a product of transpositions and for a given permutation the number of transposi tions in such a product is either always even or always odd

Proof By Theorem 11 4 we can prove the first statement by proving it for a cycle Now $(a_1 a_2 \qquad a_k) - (a\ a_2)(a\ a_3)$ $(a\ a_n)$

Now for the second statement Let $L_n - \Pi_{1\ \leq j < n}(j \quad i)$ L_n is a product of positive integers and so it is positive. Let us consider the effect upon L_n of the single transposition (k, m), where, for definiteness, we may suppose that $k < m$. The only factors of L_n which are changed in sign by (k, m) are the factors $(m - i)$ where $i \geqslant k$ and $(j - k)$ where $j \leqslant m$. Of the first type, we have $(m - (m - 1))$, $(m - (m - 2))$, . . . , $(m - k)$, of which there are $m - k$. Of the second type, different from the first, we have $((m - 1) - k)$, $((m - 2) - k)$, . . . , $((k + 1) - k)$, of which there are $m - k - 1$. Therefore, there are $2m - 2k - 1$ factors which are changed in sign, whereas all others remain unchanged. Since $2m - 2k - 1$ is odd, (k, m) changes L_n into $-L_n$. Thus, a permutation which is a product of an even number of transpositions will leave L_n unchanged, while one which is a product of an odd number of transpositions will change L_n into $-L_n$. Clearly, a given permutation, however it may be expressed, will always have the same effect on L_n. Thus, if a permutation is expressed as a product of transpositions, the number of transpositions will always be even or else always odd. ■

PROBLEM 11.14. Express the permutations of Problems 11.9, 11.10, 11.12, 11.13 in the form of Theorem 11.5 each in at least two different ways.

DEFINITION 11.6. An *even (odd) permutation* is one which can be expressed as a product of an even (odd) number of transpositions.

THEOREM 11.6. The set of all even permutations in S_n, $n > 1$, is an invariant subgroup of S_n of order $n!/2$; it is called the *alternating group of degree n, A_n*.

PROOF: If $s, t \in A_n$, then each can be expressed as a product of an even number of transpositions and so their product is also so expressible. Therefore, by condition (3) of Theorem 1.1, A_n is a subgroup of S_n.

To prove the invariance of A_n, let $s \in A_n$ and $u \in S_n$. Then s can be expressed as a product of an even number of transpositions, while u and u^{-1} together require an even number of transpositions, whether u be even or odd. Therefore, $u^{-1}su$ is expressible as a product of an even number of transpositions and so $u^{-1}su \in A_n$.

Now let $p_1, p_2, \ldots, p_k$ be the distinct permutations in A_n and let q be an odd permutation. Then $qp_1, qp_2, \ldots, qp_k$ are all odd and, since the cancellation law holds in a group, they are all different. Therefore, there are at least as many odd permutations in S_n as even ones. On the other hand, if $q_1, q_2, \ldots, q_m$ are all the distinct odd permutations in S_n, then $q_1q_1, q_1q_2, \ldots, q_1q_m$ are all even and all distinct, and so there are at least as many even permutations as odd. Therefore the number is the same and equals $n!/2$. ∎

Problem 11.15. Find A_2, A_3.

Problem 11.16. Find the composition table for A_4 (use single line notation).

Problem 11.17. Find all the subgroups of A_4, noting in particular that there is no subgroup of order 6, thus showing that the converse of Lagrange's Theorem does not hold in general.

Problem 11.18. Find all invariant subgroups of A_4, noting in particular that $H = \{1, (12)(34), (13)(24), (14)(23)\}$ is invariant (cf. Theorem 11.7).

Problem 11.19. Prove that S_n is generated by the $n - 1$ transpositions $(12), (13), \ldots, (1n)$. [Hint: $(ij) = (1j)(1i)(1j)$.]

Problem 11.20. Generalize Problem 11.19 to transpositions each of which involves any one particular k, for any k, $1 \leq k \leq n$.

Problem 11.21. Prove that A_n is generated by the 3-cycles $(123), (124), \ldots, (12n)$. [Hint: $(1i)(1j) = (1ij) = (12j)(12i)(12j)^2$.]

Problem 11.22. Generalize Problem 11.21 to 3-cycles all of which involve any 2 fixed objects.

We shall conclude our consideration of permutations with a theorem which we shall find of the utmost importance in the Galois Theory of Equations. For this we require a lemma.

Lemma. Whenever an invariant subgroup H of A_n, $n > 4$, has a 3-cycle, then $H = A_n$.

Proof. Let $(123) \in H$. Then $(123)^2 = (132) \in H$. Since H is invariant, $\sigma^{-1}(132)\sigma \in H$ $\forall\, \sigma \in A_n$. Let $\sigma = (12)(3k)$, $k > 3$. Then $\sigma^{-1}(132)\sigma = (12k) \in H$ $\forall\, k > 3$. Therefore by Problem 11.21, $A_n = H$. The details of the case when some other 3-cycle is assumed to belong to H are left to the reader. ∎

Problem 11.23. Carry out the details mentioned in the above proof. (Hint: use Problem 11.22.)

Theorem 11.7. $n > 4 \Rightarrow A_n$ is simple.

Proof. Let H be an invariant subgroup of A_n, and let $H \neq \{e\}$. We must show that $H = A_n$.

Let ρ be a permutation in $H, \rho \neq e$, which leaves fixed as many objects as possible. ρ cannot leave $n-2$ objects fixed, for then it would be an odd permutation and then $\rho \notin A_n$. Therefore, ρ must affect at least 3 objects and if we can show it affects exactly 3, the lemma will imply that $H = A_n$.

Suppose that ρ affects more than 3 objects. Then in the representation of Theorem 11.4, either (1) ρ has a cycle consisting of at least 3 objects, or (2) all the cycles are transpositions.

In the first case, we can take $\rho = (123\ldots)\ldots$, and here ρ would affect at least 5 objects, say 12345, since a 4-cycle is an odd permutation and so cannot belong to A_n. In the second case, we can take $\rho = (12)(34)\ldots$.

Now we transform by $\sigma = (345)$ and get, of course, another element of H. In the first case, $\rho_1 = \sigma^{-1}\rho\sigma = (124\ldots)\ldots$. In the second case, $\rho_1 = \sigma^{-1}\rho\sigma = (12)(45)\ldots$.

Thus in both cases, $\rho \neq \rho_1$, and so $\rho^{-1}\rho \neq e$. The permutation, $\rho^{-1}\rho_1$ leaves fixed all number > 5, since for $k > 5$, the effect of performing ρ is the same as performing ρ_1. But $\rho^{-1}\rho_1$ leaves fixed in both cases the number 1, and in the second case the number 2 as well. Therefore, $\rho^{-1}\rho_1$ leaves fixed more objects than does ρ, and $\rho^{-1}\rho_1 \in H$. Therefore, our supposition that ρ affected more than 3 objects has led to a contradiction and so it is false. Therefore, ρ is a 3-cycle and $H = A_n$. ■

COROLLARY 11.3. $n \neq 4 \Longrightarrow A_n$ is simple.

PROBLEM 11.24. Prove Corollary 11.3.

12. FINITE ABELIAN GROUPS

The problem of determining the structure of finite abelian groups has been completely solved. We now consider it. We shall use addition as the law of composition in this section and so the neutral element of the group will be denoted by 0.

THEOREM 12.1. If G is an abelian group of order $g = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, where the p_i are distinct primes, then $G = P_1 \oplus P_2 \oplus \cdots \oplus P_k$, where P_i is a subgroup in which all nonneutral elements have as periods, powers of $p_i, i = 1, 2, \ldots, k$ and the order of P_i is $p_i^{a_i}$.

PROOF: First, we shall prove that the set of all nonneutral elements having as periods, powers of p_i, and 0 form a subgroup of G, P_i. Let x and y be two such elements; i.e., $p_i^n x = 0, p_i^m y = 0$

(remember the p_i^n and p_i^m are additive exponents). Then if $q = \max(m, n)$, $p^q(x + y) = 0$. Therefore, by Theorem 1.1, these elements form a subgroup which we shall denote by P_i.

We shall now apply Theorem 7.2 with the H_i there our present P_i. Condition (1) is obviously satisfied, since G is abelian, and so is condition (3) using Lagrange's Theorem since the p_i are distinct. We must still prove that condition (2) holds. For this, let $z \in G$ and be of period $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where of course some of the b's may be zero. It easily follows by induction on the number of distinct primes actually present, by Theorem 7.1, that $z = x_1 + x_2 + \cdots + x_k$, where x_i either is the neutral element or is an element of G of period $p_i^{b_i}$. In either case, by the first part of the proof, $x_i \in P_i$, and so by Theorem 7.2, $G = P_1 \oplus P_2 \oplus \cdots \oplus P_k$. ■

Problem 12.1. Express the cyclic group of order 24 in the form given by Theorem 12.1; also the cyclic group of order 30.

Definition 12.1. A finite abelian group G *has a basis* $\Leftrightarrow \exists\, a_1, a_2, \ldots, a_n \in G \ni \forall x \in G\ \exists x_1, x_2, \ldots, x_n \in Z,\ 0 \leqslant x_i <$ period of a_i, $\ni x = x_1a_1 + x_2a_2 + \cdots + x_na_n$ and this representation is unique. The set $a_1, a_2, \ldots, a_n$ is called a *basis* of G.

Theorem 12.2. A finite abelian group G has a basis if and only if G is the direct sum of cyclic groups.

Problem 12.2. Prove Theorem 12.2.

Problem 12.3. Find bases for the abelian groups of Problem 12.1.

Theorem 12.3. A finite abelian group G is the direct sum of cyclic groups.

Proof. Since by Theorem 12.1 every finite abelian group is the direct sum of subgroups of prime power order, if we can prove the present theorem for abelian groups of order p^n we have the theorem established for all finite abelian groups.

So let G be of order p^n, where p is a prime. Let p^β be the period of an element of greatest period in G. We shall prove the theorem by induction on β.

First let $\beta = 1$, i.e., the period of every nonneutral element of G is p. Let a_1 be any element $\in G$, $a_1 \neq 0$. In case the cyclic group generated by a_1 is G we are through. If not, let $a_2 \in G$ and be such that a_2 is not in the cyclic group generated by a_1. Then the set of elements $xa_1 + ya_2$, $x = 0, 1, \ldots, p - 1$, $y = 0, 1, \ldots, p - 1$, are all dis tinct, since if two such were equal, say $xa_1 + ya_2 = ua_1 + va_2$, then $(x - u)a_1 = (v - y)a_2$, and so, since p is a prime, we should have a_2 in the subgroup generated by a_1 unless $x = u$, $y = v$. If we have now exhausted G, then G is the direct sum of the cyclic subgroups generated by a_1 and a_2. If not, the process continues. It must terminate, since G is of finite order, and when it does, we have G expressed as the direct sum of a finite number of cyclic groups of order p.

Now, suppose the theorem true for all abelian groups in which the element of highest period is p^{γ}, where $\gamma < \beta$, and let G be an abelian group in which the highest period of an element is p^{β}. Then let H be the set of all element pa, where $a \in G$. Then H is a subgroup of G since if $c = pa$, $d = pb$, $c + d = p(a + b)$. Now the highest period of an element of H is $p^{\beta-1}$, and so by the induction hypothesis and Theorem 12.2, H has a basis $a_1', a_2', \ldots, a_r'$ whose elements have periods $n_1', n_2', \ldots, n_r'$, respectively, which are, of course, powers of p. Since every element of H is of the form pa, $\exists\, a_i \in G \ni a_i' = pa_i$, $i = 1, 2, \ldots, r$ and the period of a_i is $pn_i' = n_i$.

We shall now use the a_i just obtained to get a basis of G. The $n_1n_2 \cdots n_r$ elements of G, $x_1a_1 + x_2a_2 + \cdots + x_ra_r$, $x_i = 0, 1, \ldots, n_i - 1$, are all distinct, for if two such were equal, say $x_1a_1 + \cdots + x_ra_r = y_1a_1 + \cdots + y_ra_r$, then we should have $(x_1 - y_1)a_1 + \cdots + (x_r - y_r)a_r = 0$ and not all $x_i - y_i$ zero. Now, not all the $x_i - y_i$ are divisible by p, since if they were, we could factor it out and include it with each a_i getting $(x_1 - y_1)a_1' + \cdots + (x_r - y_r)a_r' = 0$, impossible since the a_i' form a basis of H. So upon multiplying by p [by the last remark for some i, $n_i \nmid p_i(x_i - y_i)$], and we get the last equation anyway, which is impossible. Therefore, the elements are distinct.

Thus the $a_1, \ldots, a_r$ generate an abelian group K of order $n_1n_2 \cdots n_r$, which is a subgroup of G. If K is a proper subgroup of G, there exists an element $b \in G \ni b \notin K$. By hypothesis, $pb = c \in H$ and so $-c \in H$. Therefore, $-c = w_1a_1' + \cdots + w_ra_r' = p(u_1a_1 + \cdots + u_ra_r)$ and so $-c = pd$, where $d = u_1a_1 + \cdots + u_ra_r$. Consider $b + d$. Now $p(b + d) = pb + pd = c - c = 0$, and so $b + d = a_{r+1}$ is of period p and is not in K. If we add a_{r+1} to the basis elements $a_1, \ldots, a_r$ we obtain a subgroup of G which contains b. If this does not exhaust G, the process can be continued, and since G is of finite order, it must terminate after a finite number of steps. We then get a basis in which the first r elements have periods greater than p and the others all have period p.

■

Problem 12.4. Find all abelian groups of order (a) 32, (b) 81.

Corollary 12 1 A finite abelian group has a basis

Definition 12 2 The periods of the basis elements of a set of basis elements whose periods are powers of primes of a finite abelian group G are called the *invariants* of G

We might say, invariants with respect to a particular basis but by the next theorem this is unnecessary

Theorem 12 4 The invariants of a finite abelian group G are independent of the choice of basis elements

Proof We need only prove the theorem for groups whose orders are powers of a prime p

Let a_1 a_r and b_1 b_s be two bases with periods m_1 m_r and n_1 n_s respectively We may suppose them to be numbered so the $m_1 \geqslant m_2 \geqslant$ $\geqslant m_r$ and $n_1 \geqslant n_2 \geqslant$ $\geqslant n_s$ All these numbers are of course powers of the prime p Now let m_k be the first m_i which is not equal to n For definiteness suppose that $n_k > m_k$ The m_kth multiples of all the elements of G form a subgroup H which has as a basis the m_kth multiples of the elements of any the elements of any basis of G This subgroup is of course independent of the choice of basis By using the above bases of G we get the bases of H as $m_k a_1$ $m_k a_2$ $m_k a_{k-1}$ and $m_k b_1$ $m_k b_2$ $m_k b_t$ $t \geqslant k$ From the first basis the order of H is

$$\frac{m_1}{m_k} \quad \frac{m}{m_k} \qquad \frac{m_{k-1}}{m_k}$$

and from the second basis we can conclude that the order is

$$\frac{n_1}{m_k} \quad \frac{n_2}{m_k} \qquad \frac{n_k}{m_k}$$

But this last number is greater than the first We have a contradiction and so no such m_k *exists* ∎

Theorem 12 5 Two abelian groups with the same invariants are isomorphic

Theorem 12 6 For each set of powers of primes n_1 n_2 n_r there exists an abelian group with these as invariants

Problem 12 5 Prove the first statement in the proof of Theorem 12 4

Problem 12 6 Prove Theorem 12 5

PROBLEM 12.7. Describe all abelian groups of order 108 in terms of their invariants.

PROBLEM 12.8. Prove that an abelian group is cyclic if and only if its invariants are relatively prime in pairs.

PROBLEM 12.9. Find the group of automorphisms of the abelian group of order 9 and invariants 3, 3; of order 27 and invariants 3, 3, 3.

13. AUTOMORPHISMS AND ENDOMORPHISMS OF THE FOUR-GROUP, D_4

Automorphisms of D_4. We shall write D_4 as an additive group, i.e., $D_4 = \{0, a, b, a+b\}$, where $2a = 0, 2b = 0$. Its automorphisms are (in each case $0 \leftrightarrow 0$, and is omitted from the listings)

$$\iota: \begin{array}{r} a \leftrightarrow a \\ b \leftrightarrow b \\ a+b \leftrightarrow a+b \end{array} \qquad \alpha: \begin{array}{r} a \leftrightarrow a \\ b \leftrightarrow a+b \\ a+b \leftrightarrow b \end{array} \qquad \beta: \begin{array}{r} a \leftrightarrow b \\ b \leftrightarrow a \\ a+b \leftrightarrow a+b \end{array}$$

$$\gamma: \begin{array}{r} a \leftrightarrow b \\ b \leftrightarrow a+b \\ a+b \leftrightarrow a \end{array} \qquad \gamma^2: \begin{array}{r} a \leftrightarrow a+b \\ b \leftrightarrow a \\ a+b \leftrightarrow b \end{array} \qquad \delta: \begin{array}{r} a \leftrightarrow a+b \\ b \leftrightarrow b \\ a+b \leftrightarrow a \end{array}$$

It is easy to establish that $\alpha^2 = \beta^2 = \delta^2 = \gamma^3 = \iota$.

PROBLEM 13.1. Show that the above group of automorphisms is isomorphic to S_3.

Other endomorphisms of D_4. If a group G' is homomorphic to a group, G, then there exists an invariant subgroup H of G which is mapped onto e', the neutral element of G' and G/H is isomorphic to G'. Conversely, if H is any invariant subgroup of G, then G is homomorphic to G/H. (For example, the canonical homomorphism provides one such homomorphism between G and G/H, but there may be others.) Thus every homomorphic image of G can be obtained by considering G/H for every invariant subgroup H of G. Thus every endomorphism of G can be obtained by finding first all the homomorphic images of G, i.e., all quotient groups G/H, next by finding subgroups, if any, of G which are isomorphic to each G/H, and, lastly, for a particular subgroup and a particular quotient group, finding all isomorphisms between them. (This, of course, can be done by finding all automorphisms of the subgroup.)

There are five subgroups of D_4: (1) D_4 itself, (2) $\{0\}$, (3) $H_1 = \{0, a\}$, (4) $H_2 = \{0, b\}$, (5) $H_3 = \{0, a+b\}$. All are invariant.

(1) D_4/D_4 is a cyclic group of order 1. There exists exactly one such subgroup in D_4, namely $\{0\}$. So we get one endomorphism
o: $a \to 0$, $b \to 0$, $a+b \to 0$.

(2) $D_4/\{0\}$ is isomorphic to D_4. D_4 has only one subgroup isomorphic to D_4, but this subgroup has six automorphisms. So we get here the previously considered six automorphisms which, of course, are endomorphisms.

(3) D_4/H_1 is a cyclic group of order 2. D_4 has three subgroups which are cyclic groups of order 2, but each one has only the identity automorphism. Thus we have the three following endomorphisms (the only homomorphism of D_4 onto D_4/H_1 is the canonical homomorphism).

$$\begin{array}{llllll}
\epsilon & a \to 0 & \zeta & a \to 0 & \eta & a \to 0 \\
 & b \to a & & b \to b & & b \to a+b \\
 & a+b \to a & & a+b \to b & & a+b \to a+b
\end{array}$$

(4) D_4/H_2: this case is exactly like case (3) and we get the endomorphisms

$$\begin{array}{llllll}
\theta & a \to a & \kappa & a \to b & \gamma & a \to a+b \\
 & b \to 0 & & b \to 0 & & b \to 0 \\
 & a+b \to a & & a+b \to b & & a+b \to a+b
\end{array}$$

(5) D_4/H_3: this case is also like case (3) and we get the endomorphisms

$$\begin{array}{llllll}
\mu & a \to a & \nu & a \to b & \xi & a \to a+b \\
 & b \to a & & b \to b & & b \to a+b \\
 & a+b \to 0 & & a+b \to 0 & & a+b \to 0
\end{array}$$

Thus there are sixteen endomorphisms of the 4-group, of which six are automorphisms.

PROBLEM 13.2. For each of the above endomorphisms σ find the smallest positive integer $n \ni \sigma^n = \iota$, if one exists.

PROBLEM 13.3. Find all endomorphisms of C_{12}, the cyclic group of order 12. (Hint: since C_{12} is cyclic, the image of a generator determines the endomorphisms.)

PROBLEM 13.4. Find all endomorphisms of the abelian group G_8 of order 8 with invariants 2, 4.

THEOREM 13.1. The set of all endomorphisms of a group G and the usual law of composition for mappings form a subsemigroup of the semigroup of all mappings of G into itself.

Definition 13.1. If α and β are two endomorphisms of an additive abelian group G, then $\alpha + \beta$ is the mapping of G into itself determined by: $\forall x \in G, x(\alpha + \beta) = (x\alpha) + (x\beta)$.

Theorem 13.2. The set of all endomorphisms of an additive abelian group G and the addition of Definition 13.1 form an additive abelian group.

Problem 13.5. Prove Theorem 13.1. (Remember that here G is not necessarily abelian.)

Problem 13.6. Prove Theorem 13.2.

Problem 13.7. Analyze and describe the additive group of the endomorphisms of D_4.

Problem 13.8. Show that the additive group of endomorphisms of the group of Problem 13.3 is cyclic. (Hint: find an endomorphism of additive period 12.)

Problem 13.9. Do as in Problem 13.7 for the group of Problem 13.4.

14. COMPOSITION SERIES

Definition 14.1. H is a *maximal invariant subgroup* of a group, $G \Leftrightarrow$

(1) H is an invariant subgroup of G,

(2) $H \neq G$,

(3) K is an invariant subgroup of G, $K \neq H$, $K \supset H \Rightarrow K = G$.

Problem 14.1. Prove that G/H is simple if and only if H is a maximal invariant subgroup of G, $G \neq H$.

Problem 14.2. Find two distinct maximal invariant subgroups of the cyclic group of order 24: of D_8: of the cyclic group of order 60.

Theorem 14.1. M, N are maximal invariant subgroups of a group G, $M \neq N$. $D = M \cap N \Rightarrow G/M$ is isomorphic to N/D and G/N is isomorphic to M/D.

Proof: By Theorem 8.2, $M \square N$ is a subgroup of G. If $x = m \square n$ is any element of $M \square N$, then $\forall g \in G$, $g^{-1} \square (m \square n) \square g = (g^{-1} \square m \square g) \square (g^{-1} \square n \square g) = m_1 \square n_1$, where $m_1 \in M$ and $n_1 \in N$, since M, N are invariant. Therefore, $M \square N$ is invariant and contains M and N. Hence, since M, N each is maximal, $M \square N = G$.

Now the theorem follows from Theorem 4.4 by taking first $H = M$, $L = N$ and then taking $H = N$, $L = M$. ■

PROBLEM 14 3 Apply Theorem 14 1 to the groups of Problem 14 2

DEFINITION 14 2 Let $\{H_i\}$, $i = 0, 1,$ $, n+1$ be a finite sequence of subgroups of G, a group, with the following properties

(1) $H_0 = G$, $H_{n+1} = \{e\}$, where e is the neutral element of G,

(2) H_n is simple,

(3) H_{i+1} is a maximal invariant subgroup of H_i, $i = 0, 1,$ $, n$

Then and only then, the sequence $G, H_1, H_2,$ $, H_n, H_{n+1}$ is a *composition series* of the group G (also called a series of composition) The quotient groups

$$\frac{G}{H_1}\ \frac{H_1}{H_2} \qquad , \frac{H_{n-1}}{H_n}\ \frac{H_n}{e}$$

are called a set of *prime factor groups of G* and their orders, the *factors of composition* of G

THEOREM 14 2 A group of finite order has a composition series

PROBLEM 14 4 Prove Theorem 14 2

PROBLEM 14 5 Give composition series for (a) D_8, (b) C_{60}, (c) S_3 (d) S_4 (e) S_5 (f) D_4 Where possible give at least two different series

PROBLEM 14 6 Give an example of a group of infinite order which does not have a composition series

THEOREM 14 3 (Jordan–Holder) For any two composition series of a finite group G the prime factor groups are isomorphic in some order and the factors of composition are the same

PROOF The theorem is obviously true for any simple group and so it is true for any group of prime order We shall proceed by induction on the number of prime factors in the order of G Since it is true if the order is prime we shall suppose it true for all groups whose orders have fewer than n prime factors (not necessarily distinct) Now let the order of G have n prime factors and let G $M_1, M_2,$ $, M_r,$ $\{e\}$ and $G, N_1, N_2,$ $N_s, \{e\}$ be two composition series of G

If $M_1 = N_1$ the theorem then follows by induction hypothesis So let $M_1 \neq N_1$ and let $M_1 \cap N_1 = D_1$

Then by Theorem 14 1, G/M_1 is isomorphic to N_1/D_1, and G/N_1 is isomorphic to M_1/D_1 By Problem 14 1 G/M_1 and G/N_1 are simple, and since N_1/D_1 and M_1/D_1 are isomorphic to them again by Problem

14.1, D_1 is a maximal invariant subgroup of both M_1 and N_1. Now let $D_1, D_2, \ldots, D_t, \{e\}$ be a composition series for D_1. Then M_1 has the two composition series $M_1, M_2, \ldots, M_r, \{e\}$ and $M_1, D_1, \ldots, D_t, \{e\}$, and by induction hypothesis, the corresponding prime factor groups are isomorphic in some order. Therefore,

$$\frac{G}{M_1}, \frac{M_1}{M_2}, \ldots, \frac{M_r}{\{e\}} \text{ and } \frac{G}{M_1}, \frac{M_1}{D_1}, \ldots, \frac{D_t}{\{e\}}$$

are isomorphic in some order. Similarly,

$$\frac{G}{N_1}, \frac{N_1}{N_2}, \ldots, \frac{N_s}{\{e\}} \text{ and } \frac{G}{N_1}, \frac{N_1}{N_2}, \ldots, \frac{D_t}{\{e\}}$$

are isomorphic in some order. Now since G/M_1 is isomorphic to N_1/D_1 and G/N_1 is isomorphic to M_1/D_1, it is obvious that

$$\frac{G}{M_1}, \frac{M_1}{D_1}, \ldots, \frac{D_t}{\{e\}} \text{ and } \frac{G}{N_1}, \frac{N_1}{D_1}, \ldots, \frac{D_t}{\{e\}}$$

are isomorphic in some order. Therefore, by transitivity of isomorphism,

$$\frac{G}{M_1}, \frac{M_1}{M_2}, \ldots, \frac{M_n}{\{e\}} \text{ and } \frac{G}{N_1}, \frac{N_1}{N_2}, \ldots, \frac{N_s}{\{e\}}$$

are isomorphic in some order. Lastly, since isomorphic groups have the same order, the factors of composition must be the same. ■

DEFINITION 14.3. A group G is *solvable* if and only if the prime factor groups of G are of prime order.

THEOREM 14.4. A_n is solvable if $n = 3, 4$. A_n is not solvable if $n \geqslant 5$.

PROBLEM 14.7. Prove Theorem 14.4. (Hint: use Theorem 11.7.)

PROBLEM 14.8. Verify Theoıem 14.3 for the groups of Problems 14.2 and 14.5.

PROBLEM 14.9. Prove that a finite abelian group is solvable.

PROBLEM 14.10. Prove that D_{2n} and Q_{4n} are solvable.

Chapter 4: Systems with more than one Law of Composition

In the last chapter we considered primarily systems in which one law of composition was present. These systems were groups and semigroups. In the first three chapters there have been instances of systems in which more than one law of composition was defined: N, Z, the set of endomorphisms of an additive abelian group. We now consider systematically such more complicated systems. Always one law will be internal and, of the other laws, one or more may be internal or external (which we define presently) or we may have some internal and some external. We shall, however, always have some relations between the laws. One of the most important such relations is the distributive property given by Definition 5.3 of Chapter 1.

The first such system we consider is a ring, and we also consider certain special kinds of rings such as integral domains, division rings and fields. In this connection we develop the rational numbers which historically were the prototype of the concept of field just as the integers Z were the prototype of the concept of the integral domain. Then we add, for the first time, an external law of composition to get groups with operators. Continuing thus, we get to R-modules and spend considerable time on them and on a special case of them called vector spaces. This is in partial preparation for the material of Chapter 7.

The most complicated system we consider is that of an algebra and in connection with it we briefly drop the associative law.

1. RINGS, FIELDS, INTEGRAL DOMAINS

DEFINITION 1.1. A *ring* R is an additive abelian group and a second law of internal composition (which we shall write as multiplication and almost always omit the dot of multiplication) such that R and the second law form a semigroup and the right and left distributive laws of multiplication with respect to addition both hold. (The second law of internal composition need not be distinct from the first.)

As we did in the last chapter in considering additive abelian groups, we shall write the neutral element of addition as 0, and call it *zero*, and the neutral element of multiplication, if there is one, as 1 and call it the *identity element*. Inverses with respect to addition and multiplication will be written, respectively, as $-a$, a_L^{-1} (left inverse), a_R^{-1} (right inverse), *if*, of course, these latter exist.

Occasionally, one finds in the definition of a ring, the condition that the ring must have at least two elements, or that the two laws of composition be distinct. (This, by Definition 3.2 of Chapter 1, implies the existence of at least two elements.)

THEOREM 1.1. The following systems (with two internal laws of composition previously defined in each) are rings:

(1) the rational integers Z,

(2) the residue classes modulo m (an integer), Z_m,

(3) the endomorphisms of an additive abelian group G.

PROOF: The only conditions remaining to be proved are the distributive laws in (3). These we prove as follows: $\forall x \in G$, $\forall \alpha, \beta, \gamma$ endomorphisms of G, we have $x[(\alpha + \beta)\gamma] = [(x\alpha) + (x\beta)]\gamma = (x\alpha)\gamma + (x\alpha)\gamma = x(\alpha\gamma) + x(\beta\gamma) = x(\alpha\beta + \alpha\gamma) \Rightarrow (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$, and $x[\gamma(\alpha + \beta)] = (x\gamma)(\alpha + \beta) = (x\gamma)\alpha + (x\gamma)\beta = x(\gamma\alpha) + x(\gamma\beta) = x(\gamma\alpha + \gamma\beta) \Rightarrow \gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta$. ■

In addition to those properties of elements of a ring, which hold because of the properties of elements of a group or semigroup, there are some very important properties which involve both addition and multiplication. Several of these are included in the following theorem.

THEOREM 1.2. Let R be a ring. Then

(1) $\forall x \in R,\ 0 \cdot x = x \cdot 0 = 0$,

(2) $\forall x, y \in R,\ (-x)y = x(-y) = -(xy)$,

(3) $\forall x, y \in R,\ (-x)(-y) = xy$,

(4) $\forall n \in Z^+,\ \forall x \in R,\ (-x)^n = x^n$ if n is even, $(-x)^n = -x^n$ if n is odd.

PROOF: (1) $x = x + 0, x^2 = x(x + 0) = x^2 + x \cdot 0$, and so by the cancellation law of addition, $x \cdot 0 = 0$. Similarly, $0 \cdot x = 0$.

(2) $(-x)y + xy = (-x + x)y = 0 \cdot y = 0 \Rightarrow (-x)y = -(xy)$; similarly, $x(-y) = -(xy)$.

(3) and (4) are easily proved from the above [induction is needed in (4)], and so are left to the reader. ■

DEFINITION 1.2. If there exists a positive rational integer $m \ni ma = 0$ (m here is, of course, an additive exponent), $\forall a \in R$, a ring then the smallest such positive integer m is called the *characteristic* of the ring R If no such positive integer exists then R is said to be of *characteristic zero* (sometimes of characteristic infinity) (The expression "of finite characteristic" is sometimes used to mean that the ring is not of characteristic zero)

PROBLEM 1 1 Prove the statement in parentheses immediately preceding the statement of Theorem 1 1

PROBLEM 1 2 Justify each step in the part of the proof given of Theorem 1 1

PROBLEM 1 3 Describe the ring of endomorphisms of the additive 4 group the cyclic group of order 12

PROBLEM 1 4 Find the ring of endomorphisms of the additive cyclic group of order p where p is a prime Show that it is isomorphic to Z_m for some m

PROBLEM 1 5 Find the ring of endomorphisms of the additive group of Z

PROBLEM 1 6 Give a ring of each possible characteristic

PROBLEM 1 7 Show that if for any additive abelian group the product of every pair of elements is defined as zero the resulting system is a ring (This is sometimes called a *zero ring*)

DEFINITION 1 3 $a \neq 0$ $a \in R$ a ring a is a *left (right) divisor of zero* $\Leftrightarrow \exists\, b \in R$ $b \neq 0$ $\ni a \;\; b = 0$ ($b \;\; a = 0$) a is a *regular element* of a ring $R \Leftrightarrow a \neq 0$ $a \in R$ a is not a divisor of zero

Sometimes divisors of zero as defined above are called proper divisors of zero

THEOREM 1 3 Let $a \in R$ a ring The cancellation laws of multiplication hold for $a \Leftrightarrow a$ is a regular element

PROBLEM 1 8 Prove Theorem 1 3

PROBLEM 1 9 Prove that a unit (cf Definition 16 2 of Chapter 2) is regular

PROBLEM 1 10 Find two rings in which all nonzero elements are regular

PROBLEM 1 11 Find which of the rings so far considered contain (a) identity elements, (b) units (c) divisors of zero

PROBLEM 1.12. Prove in a ring R of finite characteristic and with an identity element, that the additive period of the identity element is the characteristic of the ring.

DEFINITION 1.4. S is a *subring* of a ring $R \Leftrightarrow$

(1) $S \subset R$,

(2) $\langle S, +\rangle$ is a subgroup of $\langle R, +\rangle$,

(3) $\langle S, \cdot\rangle$ is a subsemigroup of $\langle R, \cdot\rangle$.

DEFINITION 1.5. Two elements of a ring R are *permutable* if and only if they are permutable under multiplication. A ring R is *commutative* if and only if multiplication in R is commutative.

PROBLEM 1.13. Show that every ring except one particular ring (and all others isomorphic to it) has at least two subrings.

PROBLEM 1.14. Prove that the set C of all elements of a ring R which are permutable with all elements of R is a subring of R.

There are certain kinds of rings in which the multiplicative semigroup has further properties. Some of these we define now.

DEFINITION 1.6. An *integral domain* (also called a *domain of integrity*) is a commutative ring I with an identity element $\neq 0$, in which all nonzero elements are regular.

A *division ring* is a ring D in which the nonzero elements form a group. (This is sometimes called a field, or a sfield.)

A *field* is a commutative division ring. (When a division ring is called a field, this is called a commutative field.)

PROBLEM 1.15. Prove that a field is an integral domain.

PROBLEM 1.16. Prove that Z_m is a field if and only if m is a prime.

PROBLEM 1.17. Find which rings considered so far are integral domains and which are fields.

PROBLEM 1.18. Prove that a finite integral domain is a field.

DEFINITION 1.7. The *ring product* of two rings R and S is the set product $R \times S$ with addition defined as in the group product of the additive groups of the rings, and multiplication defined as in the semigroup product of the multiplicative semigroups of the rings.

THEOREM 1.4. The ring product of two rings is a ring.

PROBLEM 1.19. Prove Theorem 1.4.

PROBLEM 1.20. Find an example of a ring product of two fields which is not a field (Hint: look for divisors of zero). Then prove that the ring product of two fields is *never* a field.

Since we know from Theorem 12.8 of Chapter 2 that a commutative semigroup in which the cancellation law holds for every element can be imbedded in a group, the question naturally arises as to whether an integral domain can be imbedded in a field. If we omit commutativity but keep all other properties, the ring cannot necessarily be imbedded in a division ring. [This was shown by A. Malcev, *Math. Ann.* Vol. CXIII, p. 686 (1936).] However, for an integral domain, it is possible. First of all we make clear what is meant by having one ring imbedded in another. For this we generalize Definitions 11.1 and 11.2 of Chapter 2. Presently we shall give generalizations of these two definitions, so at present we shall merely say that two rings, R and S, are isomorphic if and only if there exists a 1–1 mapping α of R onto S such that α is an isomorphism of the additive groups and an isomorphism of the multiplicative semigroups. Then the ring R is imbedded in the ring T if and only if there exists a subring S of T and an isomorphism α of R onto S. In general, of course, there may be more than one such isomorphism between R and S. This gives us an opportunity, when present, to select the one best suited to our purposes. Also there may be more than one subring of T which is isomorphic to R. Again, we may be able to choose the one we want.

THEOREM 1.5. I is an integral domain $\Rightarrow \exists$ a field F in which I is imbedded.

PROOF. Much of the proof is similar to the developments in Chapter 2, beginning with Theorem 12.7.

Let I^* be I with 0 removed, and let $K = I \times I^*$. We define addition and multiplication in K as follows: $(a_1, a_2) + (b_1, b_2) = (a_1b_2 + a_2b_1, a_2b_2)$, $(a_1, a_2) \cdot (b_1, b_2) = (a_1b_1, a_2b_2)$. We leave to the reader the simple verification that K and each of these laws form a commutative semigroup and that multiplication is distributive with respect to addition, as well as the verification that the relation R, defined by $(a_1, a_2) R (b_1, b_2) \Leftrightarrow a_1b_2 = a_2b_1$, is an equivalence relation compatible with addition and multiplication as just defined in K. Then by Theorem 12.1, and those following it in Chapter 2, we have K/R closed with respect to each of the induced laws $\bar{+}$ and $\bar{\cdot}$, that each of these laws is associative and commutative, and that $\bar{\cdot}$ is distributive with respect to $\bar{+}$.

Further, if we let $C_{(a,b)}$ denote the equivalence class (with respect to R) containing (a, b), we have $C_{(0,1)} \bar{+} C_{(a_1,a_2)} = C_{(0\ a_2+1\ a_1,\ 1\ a_2)} = C_{(a_1,a_2)} = C_{(a_1,a_2)} \bar{+} C_{(0,1)}$ so $C_{(0,1)}$ is a zero element; also $C_{(a,b)} \bar{+} C_{(-a,b)} = C_{(ab-ab,b^2)} = C_{(0,1)}$. Thus K/R is a commutative ring. Further, $C_{(a,b)} \bar{\cdot} C_{(1,1)} = C_{(a\cdot 1, b\cdot 1)} = C_{(a,b)} = C_{(1,1)} \bar{\cdot} C_{(a,b)}$. So $C_{(1,1)}$ is an identity element. Now $C_{(a,b)} \neq 0 \Leftrightarrow a \neq 0$, and so if $C_{(a,b)} \neq 0$, then $C_{(a,b)} \bar{\cdot} C_{(b,a)} = C_{(1,1)}$, and since $C_{(b,a)} \in K/R$, each element of K/R which is not $C_{(0,1)}$ has an inverse. Therefore, K/R is a field.

Now it is immediate that the set of all $C_{(x,1)}$, $\forall\ x \in I$ is a subring of K/R. We shall show that the mapping α defined by $x\alpha = C_{(x,1)}$ is an isomorphism of I onto this subring. It is clearly an *onto* mapping. If $C_{(x,1)} = C_{(y,1)}$, then, by the definition of R, $x \cdot 1 = 1 \cdot y \Rightarrow x = y$ and so α is 1–1. Now $(x + y)\alpha = C_{(x+y,1)} = C_{(x,1)} \bar{+} C_{(y,1)} = x\alpha \bar{+} y\alpha$. Also $(xy)\alpha = C_{(xy,1)} = C_{(x,1)} \bar{\cdot} C_{(y,1)} = (x\alpha) \bar{\cdot} (y\alpha)$. Therefore, α is an isomorphism and so I is imbedded in the field $F = K/R$. ■

THEOREM 1.6. Every field L containing the integral domain I as a subring contains the field F of Theorem 1.5.

PROOF: For the proof of this theorem it is sufficient to show that every element of F is a quotient of two elements of I, since every field containing I must contain all such quotients.

Now $C_{(a,b)} = C_{(a,1)} \bar{\cdot} C_{(1,b)} = C_{(a,1)} \bar{\cdot} C_{(b,1)}{}^{-1} = C_{(a,1)}/C_{(b,1)}$, this form being permitted since multiplication is commutative. ■

DEFINITION 1.8. The field $F = (I \times I')/R$ of Theorems 1.5 and 1.6 is called the *field of quotients* of the integral domain I. If $I = Z$, we shall denote the field of quotients by Q, call it the *field of rational numbers*, and call its elements, *rational numbers*.

PROBLEM 1.21. Show that the field F of Theorems 1.5 and 1.6 is the smallest field containing I.

PROBLEM 1.22. Show that any ring R can be imbedded in a ring with an identity element. [Hint: consider $Z \times R$, and define: $(m, a) + (n, b) = (m + n, a + b)$, $(m, a) \cdot (n, b) = (mn, na + mb + ab)$.]

2. LAWS OF EXTERNAL COMPOSITION AND GROUPS WITH OPERATORS

DEFINITION 2.1. A *law of external composition* between elements of a set Ω, frequently called the set of operators, and elements of a set S, is a mapping of a part A of $\Omega \times S$ into S. If $A = \Omega \times S$, then we say that the law is defined everywhere and S is *closed* with respect to (or under) the law.

EXAMPLE 2.1. Let $\Omega = N$ and S be a semigroup. Then the mapping $(n, s) \to s^n$ is an external law of composition for S ($n \in N$, $s \in S$).

EXAMPLE 2.2. Let $S = G$, a group and Ω be any set of endomorphisms of G. Then $(\theta, g) \to g\theta$ $\forall \theta \in \Omega$ is an external law for G.

EXAMPLE 2.3. Let $S = \{a\}$ and Ω be any set whatsoever. Then $(\omega, a) \to a$ $\forall \omega \in \Omega$ is an external law for S.

In Definition 2.1 and in Example 2.3 the sets S and Ω had no properties except those demanded by Definition 2.1. In Examples 2.1 and 2.2 the sets involved did have other properties, namely laws of internal composition defined in them. When we add conditions of this kind we get various types of algebraic systems. The first such involves an internal law in S but none in Ω.

DEFINITION 2.2. A set G, a law of internal composition $\square$ and a law of external composition Δ with set of operators M form a *group with operators* (or an M group) $\Leftrightarrow$

(1) G, $\square$ form a group

(2) G is closed with respect to Δ, M

(3) $\forall a, b \in G$, $\forall \theta \in M$, $(a \square b) \Delta \theta = (a \Delta \theta) \square (b \Delta \theta)$

For brevity we shall frequently refer to a group with operators by the single letter denoting the set in which the internal law is defined.

Since the symbol for the external law Δ is placed between elements of sets which are usually different, no ambiguity can result from omitting Δ and merely writing the elements adjacent to each other. We shall henceforth usually do this, and then condition (3) of Definition 2.2 in part becomes $(a \square b)\theta = (a\theta) \square (b\theta)$.

When we refer to G as the group G without operators, we shall mean the group determined in condition (1) of Definition 2.2. When we refer to subgroups, normal subgroups, etc., of a group with operators, we mean that the sets in question are subgroups, etc., of the group without operators. We now introduce further terminology for subsets peculiar to a group with operators.

DEFINITION 2.3. Let G be a group with operators M.

An element $a \in G$ is *invariant* for an operator $\theta \in M \Leftrightarrow a\theta = a$.

A subgroup H of G is a *stable subgroup* (also called admissible or an M group) $\Leftrightarrow \forall h \in H$, $\forall \theta \in M$, $h\theta \in H$.

An operator $\epsilon \in M$ is called a *neutral operator* $\Leftrightarrow \forall a \in G$, $a\epsilon = a$.

From condition (3) of Definition 2.2 we see that every operator of a group with operators provides an endomorphism of G as a group without operators. Thus a group with operators may be regarded as a group and a set of endomorphisms of the group. For example, we may consider the 4-group and the endomorphisms designated in the previous chapter by o, ζ, ϵ. This is a group with operators and one stable subgroup is H_1, as an inspection of the endomorphisms concerned immediately shows, while H_2 and H_3 are not stable subgroups.

PROBLEM 2.1. Using the 4-group as above and the endomorphisms, $o, \iota, \alpha, \epsilon, \zeta$, find the stable subgroups.

PROBLEM 2.2. Do the same as in Problem 2.1 using all endomorphisms.

PROBLEM 2.3. Find the stable subgroups of the additive cyclic group of order 12 and all its endomorphisms.

PROBLEM 2.4. For the group with operators consisting of a group G and all its inner automorphisms, find all stable subgroups.

PROBLEM 2.5. For a ring R show that the additive group of R and operators consisting of all elements of R with multiplication as defined in R as the external law between operators and elements of the additive group of R form a group with operators.

PROBLEM 2.6. Let $R = Z$ in Problem 2.5, and find all stable subgroups; do the same with $R = Q$.

PROBLEM 2.7. Let G be an abelian group and $M = Z$, and let the external law be $(n.g) \rightarrow g^n$, $\forall\, n \in Z$, $\forall\, g \in G$. Prove that the resulting system is a group with operators. Find some stable subgroups.

PROBLEM 2.8. Let R be a commutative ring. Prove that the additive group of the ring product $R \times R$, with operators $r \in R$ and external law $r(r_1, r_2) = (rr_1, rr_2)$ is a group with operators. Find some stable subgroups.

PROBLEM 2.9. For the system of Problem 2.8, let R be a field F. Find some stable subgroups H with the additional property that $\forall\, r \in F, r \neq 0, rH = H$.

PROBLEM 2.10. Prove that Theorems 3.1 and 3.2 of Chapter 3 hold if, for "group" we substitute "group with operators" and for "subgroup," "stable subgroup."

3. ALGEBRAIC SYSTEMS AND HOMOMORPHISMS

Since we have now considered both internal and external laws of composition defined on a set, and since we have considered sets on which two such laws are defined, the reader can appreciate the desirability of some general definitions pertaining to such sets and laws. So we now give these definitions.

DEFINITION 3.1. (Cf. 4.1 of Chapter 2.) Let Δ be a law of external composition defined in a set S with operators Ω and T be a subset of S. Then the *restriction of* Δ *to* T is the law of external composition defined in T by the restriction (cf. Definition 3.4 of Chapter 1) to $\Omega \times T$ of the mapping determining Δ in T.

DEFINITION 3.2. (1) An *algebraic system* is a set S and one or more laws of internal composition defined in S and no, one, or more laws of external composition defined between elements of a set or several sets of operators and elements of S. Further, these laws may be subjected to fulfilling certain conditions (e.g., commutativity, associativity, etc.) and to satisfy certain relations between the laws (e.g., distributivity).

(2) Two algebraic systems with the same number of internal laws, the same number of external laws, with a 1-1 mapping of the laws of one system onto the laws of the other system such that corresponding laws satisfy the same conditions and the same relations, are said to be of the *same species*.

(3) Two algebraic systems of the same species are *homologous* if and only if the sets of operators for corresponding laws of the two systems are the same.

(4) An algebraic system T is a *subsystem* of an algebraic system S if and only if (a) $T \subset S$, (b) T is closed with respect to each law of composition (internal and external) of S, (c) each law of composition of T is obtained as a restriction to T of a law of composition of S.

PROBLEM 3.1. Certain subsets of the algebraic systems so far considered have been given special names. Determine which of these are subsystems in accordance with Definition 3.2 (4).

DEFINITION 3.3. Let $\{S_\alpha\}$, $\alpha \in \Lambda$, be a collection of homologous algebraic systems. Then their *product* $\Pi_{\alpha \in \Lambda} S_\alpha$ is their set product (cf. Definition 4.2 of Chapter 1) with the following laws of composition:

(1) for each law of internal composition $\square^{\alpha}_{i}$, $\alpha \in \Lambda$, $i = 1, \ldots, n$, we define $\square_i$ by

$$\{s_\alpha\}_{\alpha\in\Lambda}\,\square_i\,\{t_\alpha\}_{\alpha\in\Lambda} = \{s_\alpha\,\square_i^{(\alpha)}t_\alpha\}$$

(2) for each law of external composition, $\Delta_i^{(\alpha)}$, we define

$$\Theta\,\Delta_i\,\{s_\alpha\}_{\alpha\in\Lambda} = \{\Theta\,\Delta_i^{(\alpha)}\,s_\alpha\}_{\alpha\in\Lambda},\ i=1,\ldots,n,\ \alpha\in\Lambda.$$

for each operator Θ.

PROBLEM 3.2. Show that semigroup product, group product, and ring product are special cases of Definition 3.3.

PROBLEM 3.3. Prove that the product of homologous algebraic systems is an algebraic system homologous to the given ones.

DEFINITION 3.4. Let S and S' be two homologous algebraic systems with laws $\square_i$, Δ_i and $\square_i'$, Δ_i', respectively. Then a mapping α of S into S' is a homomorphism of S into S' $\Leftrightarrow$

(1) $(s_1\,\square_i\,s_2)\alpha = (s_1\alpha)\square_i'\,(s_2\alpha)$, $\forall\ i$, and $\forall\ s_1, s_2 \in S$

(2) $(\Theta\,\Delta_i s)\alpha = \Theta\,\Delta_i'\,(s\alpha)$, $\forall i$, $\forall\ s \in S$, and for each operator Θ.

α is a homomorphism of S *onto* S' if and only if α is a homomorphism of S into S' and α maps S onto S'. Then we say that S' is homomorphic to S.

If α is, further, 1–1, α is an *isomorphism* of S onto S', and so we say that S and S' are *isomorphic*.

If $S = S'$, then if α is a homomorphism, we call it an *endomorphism*, and if α is an isomorphism, an *automorphism*.

An algebraic system S is *imbedded* in a homologous algebraic system $U \Leftrightarrow \exists$ a subsystem T of $U \in S$ and T are isomorphic.

The above definitions of course apply to groups with operators. It should be noted that, according to Definition 3.4, the endomorphisms of a group with operators are precisely those endomorphisms of the group without operators which are permutable with all the endomorphisms of the group without operators which are operators.

PROBLEM 3.4. Find the endomorphisms of the group with operators of Problem 2.1.

PROBLEM 3.5. Do the same as Problem 3.4, for the group of Problem 2.3.

Naturally all theorems about groups with operators hold for groups without operators, since M of Definition 2.2 may be empty.

On the other hand, many, but not all theorems about groups without operators generalize to groups with operators. One place where it is necessary to clarify such generalization is in connection with quotient groups Let G be a group with operators M and H a stable invariant subgroup of G We wish to have the quotient group G/H be a group with operators To do this we must define $A\Theta$ for all $A \in G/H$ and for all $\Theta \in M$ and the definition of it must make it an element of G/H To define $A\Theta$ as might be suggested by the obvious generalization of Definition 3 1 of Chapter 3 (i e to define it as the set of all $a\Theta$ for all $a \in A$) is unsatisfactory since even if $A = H$ we may have $H\Theta \neq H$ with that generalization (of course $H\Theta \in H$ since H is stable) and so the composite would not be an element of G/H To avoid this difficulty we define $A\Theta$ to be the coset $B \ni a\Theta \in B$ $\forall\, a \in A$ By condition (3) of Definition 2 2 and by Definition 3 4 this makes G/H a group with operators M

PROBLEM 3 6 Fill in the details of the proof of this last statement

PROBLEM 3 7 Take a stable subgroup of the group of Problem 2 1 and describe the quotient group corresponding to it

PROBLEM 3 8 Generalize Theorems 3 6 3 7 3 8 3 9 3 10 and 3 12 of Chapter 3 to groups with operators

4 MODULES

Now we consider groups with operators and start adding conditions to the set of operators and this will require some relations between the various laws of composition present

DEFINITION 4 1 Let R be a ring Then an additive abelian group E with operators R is a ***left R module*** $\Leftrightarrow$

(1) $\forall \alpha\ \beta \in R\ \ \forall x \in E\ \ (\alpha + \beta)x = \alpha x + \beta x$

(2) $\alpha(\beta x) = (\alpha\beta)x$

If (2) is replaced by

$$(2)\quad \alpha(\beta x) = (\beta\alpha)x$$

then E is a *right R module*

An R module E (either left or right) is *unitary* if and only if R has an identity element ϵ which is a neutral operator i e $\forall\, x \in E$ $\epsilon x = x$

If it is clear from the context whether E is a right or a left R module or if it doesn t matter then the simpler expression R module will be used This will always be the case if R is commutative

It should be noted in condition (1) of the above definition that the + sign on the left denotes addition in R, while the + sign on the right denotes addition in E. Also, in condition (2) we have multiplication of elements of R and multiplication between an element of R and an element of E. No confusion should result from this. It should be noted that an R-module involves four laws of composition.

Problem 4.1. Prove that in an R-module E, (a) $\forall\, \alpha \in R$, $\alpha \cdot 0 = 0$, (b) $\forall\, x \in E$, $0 \cdot x = 0$, (c) $\forall\, \alpha \in R$, $\forall\, x \in E$, $\alpha(-x) = (-\alpha)x = -(\alpha x)$. Interpret the zeros and the minus signs carefully.

We now define a particular R-module which is of fundamental importance.

Definition 4.2. If R is a ring, then $V_n^L(r)$ is the additive group of the ring product of n factors, all equal to R, with operator product defined as $r(r_1, r_2, \ldots, r_n) = (rr_1, rr_2, \ldots, rr_n)$, $\forall\, r \in R$. $V_n^R(R)$ is the same except that $r(r_1, r_2, \ldots, r_n) = (r_1 r, r_2 r, \ldots, r_n r)$. In $x = (r_1, r_2, \ldots, r_n)$, r_i is called the *ith component* of x. If R is commutative, or if from the context the meaning is clear, $V_n^l(R)$ or $V_n^R(R)$ will be denoted simply by $V_n(R)$.

Theorem 4.1. $V_n^l(R)$, $(V_n^R(R))$ is a left (right) R-module. If R has an identity element, both $V_n^l(R)$ and $V_n^R(R)$ are unitary.

Definition 4.3. E is a *vector space* over the field $F \Leftrightarrow E$ is a unitary F-module where F is a field.

Definition 4.4. A *submodule (vector subspace)* of an R-module (vector space E over F) is a subsystem of E [cf. Definition 3.2(4)] which is an R-module (vector space over F).

Problem 4.2. Prove Theorem 4.1.

Problem 4.3. Show that $V_n(Z)$ is a Z-module, which is a subset but *not* a submodule of $V_n(Q)$.

Problem 4.4. Show that if S is a subring of a ring R, then every submodule of an R-module is an S-module.

Problem 4.5. Show that in a unitary R-module E, the mapping $\forall\, x \in E$, $x \to \alpha x$, where α is a unit of R, is an automorphism of the additive group (without operators) E.

Problem 4.6. Show that in a vector space E over F, the mapping, $\forall\, x \in E$, $x \to \alpha x$ is an automorphism of the additive group (with operators) E, for every $\alpha \neq 0$, $\alpha \in F$.

Problem 4 7 Prove that if M N are two submodules of an R module E then $M + N$ and $M \cap N$ are submodules of E

Problem 4 8 Prove that every submodule of a vector space E is a subvector space of E

The quotient module of an R module is a special case of the quotient group of a group with operators

The module product of R modules is covered by Definition 3 3 and Problem 3 3 establishes that it is an R module If we have a collection of R modules $\{E_\iota\}$ $\iota \in \Omega$ then the module product in the case that each E_ι is the additive group of R with R as the set of operators (cf Problem 2 5) is denoted by R_l^{Ω} or R_R^{Ω} according as operator multiplication is on the left or right If $\Omega = \{1\ 2\ \ldots\ n\}$ then $R_l^{\Omega}(R_R^{\Omega})$ is denoted more briefly by $R_l^{n}(R_R^{n})$ and coincides of course with $V_n(R)(V_n'(R))$

We now generalize Definition 7 2 of Chapter 3 to R modules

Definition 4 5 Let M_1 M_2 be submodules of the R module E Then E is the *direct sum* written $E = M_1 \oplus M_2$ if and only if

(1) $M_1 \cap M_2 = \{0\}$

(2) every element of E can be expressed uniquely as $x + y$ where $x \in M_1$ $y \in M_2$

Further we say that the submodules M_1 M_2 of E are *supplementary* $\Leftrightarrow E = M_1 \oplus M_2$

Problem 4 9 Prove that if E is a unitary R module so is E/M where M is a submodule of E

Problem 4 10 Prove that every module quotient of a vector space is a vector space

Problem 4 11 Let M be those elements of $V_2(Z)$ of the form $(0\ b)$ $\forall b \in Z$ Show that M is a submodule of $V_2(Z)$ and that $V_2(Z)/M$ is isomorphic to Z

Problem 4 12 Let M be the set of those elements of $V_3(Z)$ of the form $(0\ b\ c)$ $\forall b\ c \in Z$ and let N be the set of those elements of $V_3(Z)$ of the form $(a\ 0\ 0)$ $\forall a \in Z$ Show that M and N are submodules of $V_3(Z)$ that $V_3(Z)/M$ is isomorphic to N and that $V_3(Z)/N$ is isomorphic to M

Problem 4 13 Show that the submodules of Problem 4 12 are supplementary

Problem 4 14 Show that in Z considered as a Z module the submodule consisting of the even integers does not have a supplementary submodule.

Theorem 4.2. Let M_1, M_2 be submodules of the R-module E. Then $E = M_1 \oplus M_2 \Rightarrow E$ is isomorphic to the module product of M_1 and M_2.

Theorem 4.3. If $E = M_1 \oplus M_2$, then the mapping, $\forall\, x \in M_2$, $x \to$ (the equivalence class of E with respect to M_1 containing x) is an isomorphism between E/M_1 and M_2.

Problem 4.15. Prove Theorem 4.2.

Problem 4.16. Prove Theorem 4.3.

Problem 4.17. Generalize Definition 4.3 and Theorem 4.2 to a direct sum of n modules. Prove the latter.

We conclude this paragraph by stating a theorem whose proof is immediate by induction and is left to the reader.

Theorem 4.4. Let $\{x_k\}, \{y_k\}, k = 1, 2, \ldots, n$ be two finite sequences of elements of an R-module E. Then

(1) $\sum_{k=1}^{n} (x_k + y_k) = \sum_{k=1}^{n} x_k + \sum_{k=1}^{n} y_k$,

(2) $\alpha \sum_{k=1}^{n} x_k = \sum_{k=1}^{n} \alpha x_k, \forall\, \alpha \in R$.

5. LINEAR DEPENDENCE IN AN R-MODULE

Definition 5.1. Let E be an R-module. Then $x \in E$ is a *linear combination* with coefficients $\in R$ of elements of the set $A \subset E \Leftrightarrow \exists\, \lambda_k \in R, a_k \in A, k = 1, 2, \ldots, n, \ni x = \sum_{k=1}^{n} \lambda_k a_k$. The λ_k are called the *coefficients*. The element x is, under these circumstances, said to be *linearly dependent over* R, on $a_1, a_2, \ldots, a_n$.

Example 5.1. Let $E = V_2(Z)$, $A = \{(3,4), (-3,7), (5,8)\}$. Then $(-3, -8)$ is a linear combination over Z of elements of A since $(-3,-8) = 4(3,4) + (-3)(5,8) = 4(3,4) + 0(-3,7) + (-3)(5,8)$.

Example 5.2. Let $E = Z$, considered as a Z-module, $A = \{8, 12\}$. Then 4 is a linear combination over Z of elements of A since $4 = (-4)(8) + (3)(12)$.

Problem 5.1. Describe the set of all linear combinations in Z of 3; of 4, 6; of 4, 5.

Problem 5.2. Prove that the set of all linear combinations of $(1, 0)$ and $(0, 1)$ as elements of $V_2(R)$ is $V_2(R)$ for any ring R which has an identity element.

PROBLEM 5.3. Prove that the set of all linear combinations of (3, 4) and (4, 5) as elements of $V_2(Q)$ is $V_2(Q)$.

PROBLEM 5.4. Do Problem 5.3 in $V_2(Z)$.

PROBLEM 5.5. Prove that the set of all linear combinations of (2, 4) and (4, 5) as elements of $V_2(Z)$ is not $V_2(Z)$.

PROBLEM 5.6. Generalize Problem 5.2 to $V_n(R)$, where R is a ring with an identity element.

THEOREM 5.1. Let $A \subset E$, an R module. The set M of all linear combinations with coefficients in R of elements of the set A is a submodule of E, i.e., an R module. Let S be a subring of R. Then the set N of all linear combinations with coefficients in S of elements of A is an S module.

PROOF. This theorem follows immediately from Theorem 4.4. ∎

COROLLARY 5.1. As in Theorem 5.1, let L be any submodule of E containing A. Then $L \supset M$.

DEFINITION 5.2. Let $A \subset E$, an R module. *The submodule of E generated by A* is the smallest (cf. Definition 1.7 of Chapter 3) submodule of E containing A.

COROLLARY 5.2. If E is a unitary R module and $A \subset E$, then the submodule generated by A is the module M of Theorem 5.1 and each element is of the form $r_1a_1 + \cdots + r_ka_k$, where $r_i \in R$ and $a_i \in A$, $i = 1, 2, \ldots, k$.

COROLLARY 5.3. If E is not a unitary R module and $A \subset E$, then the submodule generated by A contains properly the module M of Theorem 5.1 and each element is of the form $r_1a_1 + \cdots + r_ka_k + n_1a_1 + \cdots + n_ma_m$, where $r_i \in R$, $a_i \in A$, $n_i \in Z$.

PROBLEM 5.7. Describe the Z module generated by the two elements of Problem 5.5; the Z module in Z generated by 5, by 1, by 3, and by 5.

PROBLEM 5.8. If R is the ring of even integers, describe the module generated by 4, by 8.

DEFINITION 5.3. The elements of a set A of an R module E are *linearly independent over R* $\Leftrightarrow$ $(\sum_{i=1}^{k} \lambda_i a_i = 0$, $\lambda_i \in R$, $a_i \in A \Rightarrow$

$\lambda_i = 0$ for $i = 1, \ldots, n$). The set A is then called *free*. The elements $a_1, a_2, \ldots, a_n \in E$ are *linearly dependent over* $R \Leftrightarrow \exists \lambda_i \in R$, with some one or more $\lambda_i \neq 0 \ni \sum_{i=1}^{n} \lambda_i a_i = 0$.

In a general R-module, there is an important distinction between Definitions 5.1 and 5.3, for it is possible to have the elements of a set linearly dependent without having any one of the elements expressible as a linear combination of the others. For example, in Z considered as a Z-module, 2 and 5 are linearly dependent since $(5) \cdot 2 + (-2) \cdot 5 = 0$, but there is no element $\lambda \in Z \ni 5 = \lambda \cdot 2$, nor any $\mu \in Z \ni 2 = \mu \cdot 5$. However, the situation changes if the nonzero elements of R have inverses.

THEOREM 5.2. Let E be a unitary D-module, where D is a division ring, and let $a_1, a_2, \ldots, a_n$ be a set of nonzero elements of E which are linearly dependent. Then $\exists$ at least one $a_k \ni a_k$ is linearly dependent on the others.

PROOF: By Definition 5.3, $\exists \lambda_i \in D$, with some $\lambda_k \neq 0 \ni \sum_{i=1}^{n} \lambda_i a_i = 0$. Then $\lambda_k a_k = -\lambda_1 a_1 - \cdots - \lambda_{k-1} a_{k-1} - \lambda_{k+1} a_{k+1} - \cdots - \lambda_n a_n$. Now since $\lambda_k \neq 0$, and D is a division ring, λ_k^{-1} exists and so $a_k = \mu_1 a_1 + \cdots + \mu_{k-1} a_{k-1} + \mu_{k+1} a_{k+1} + \cdots + \mu_n a_n$, where $\mu_i = -\lambda_k^{-1} \lambda_i$.

COROLLARY 5.4. Under the conditions of Theorem 5.2, at least two of the a_i are linearly dependent on the others.

PROBLEM 5.9. Prove Corollary 5.4.

PROBLEM 5.10. Prove that in any R-module if x is linearly dependent on $a_1, \ldots, a_n$, then the elements $x, a_1, \ldots, a_n$ are linearly dependent, if R is not a zero-ring.

PROBLEM 5.11. Determine which of the following sets of elements are linearly dependent:

(a) over Z, as elements of $V_4(Z)$; (i) $(1, 3, 4, 7)$, $(-2, -6, -8, -14)$; (ii) $(4, -2, -6, -10)$, $(-6, 3, 9, -15)$; (iii) $(1, 3, 4, 7)$, $(4, -2, -6, 10)$ $(11, 5, 0, 41)$.

(b) over Z_6, as elements of $V_3(Z_6)$; (i) $(1, 2, 4)$, $(2, 4, 3)$; (ii) $(1, 2, 4)$, $(3, 0, 0)$; (iii) $(2, 2, 4)$.

PROBLEM 5.12. Show that the following elements of $V_4(Z)$ are linearly independent: $(1, 3. 4, 7)$, $(-2, -6, -8, -13)$.

PROBLEM 5.13. Show that in $V_n(R)$, where R is a ring with an identity element, the elements e_i, with the ith component 1, and all other components zero, are linearly independent.

Definition 5.4 A *basis* of a unitary R module E is a free set of elements which generate E. A unitary R module with a basis is called a *free module*.

Problem 5.14 Show that the e_i of Problem 5.13 form a basis of $V_n(R)$.

Theorem 5.3 Let R be a ring with an identity element. Then a unitary R module E has a finite basis $\Leftrightarrow$ E is isomorphic to some $V_n(R)$.

Problem 5.15 Prove Theorem 5.3. (Hint: by hypothesis E has a finite basis, say $a_1, \dots, a_n$. By Problem 5.14 e_i, $i = 1, \dots, n$ form a basis of $V_n(R)$. Prove that the mapping $a_i \leftrightarrow e_i$ determines an isomorphism between E and $V_n(R)$.)

6 VECTOR SPACES

In this section we shall prove the important properties of linear dependence and independence in a vector space. At the end of the section are a number of exercises which are easy to prove using the properties of linear dependence and which give important properties of vector spaces.

Theorem 6.1 $u_1, \dots, u_n \in E$, a vector space over F, are linearly independent $\Rightarrow$ each subset of $u_1, \dots, u_n$ is free.

Proof Suppose $u_{k_1}, \dots, u_{k_s}$ were linearly dependent. Then $\exists$ $\lambda_{k_j} \in F \ni \sum_{j=1}^{s} \lambda_{k_j} u_{k_j} = 0$ with not all $\lambda_{k_j} = 0$. Then let $\mu_i = 0$ for $i \neq k_1, \dots, k_s$, $\mu_{k_j} = \lambda_{k_j}$ for $j = 1, 2, \dots, s$. Then $\sum_{j=1}^{n} \mu_j u_j = 0$ and not all $\mu_j = 0$. ■

Theorem 6.2 If $v \in E$, a vector space over F, is linearly dependent on $u_1, \dots, u_k \in E$ but not on $u_1, \dots, u_{k-1}$, then u_k is linearly dependent on $u_1, \dots, u_{k-1}, v$ and the subspace generated by $u_1, \dots, u_k$ is the same as the subspace generated by $u_1, \dots, u_{k-1}, v$.

Proof By hypothesis we have $v = \sum_{i=1}^{k} \lambda_i u_i$ with $\lambda_k \neq 0$. Then $u_k = \sum_{i=1}^{k-1} (-\lambda_k^{-1} \lambda_i) u_i + \lambda_k^{-1} v$. The result now follows from Theorem 5.1. ■

Theorem 6.3 In E, a vector space over F, let $v_1, \dots, v_s$ be linearly independent and let $v_j \in M$, the subspace generated by $u_1, \dots, u_n$, which are linearly independent elements of E. Then there exists a set $u_{i_1}, u_{i_2}, \dots, u_{i_s}$ such that the subspace generated by the set obtained from $u_1, \dots, u_n$ by replacing u_{i_j} by v_j is M. Thus $s \leqslant n$.

PROOF: We proceed by induction. If $s = 1$, the result follows from Theorem 6.2 by renumbering the u's if necessary.

Suppose that the theorem is true for $(s - 1)$ v's and consider s v's. The system arising by replacing suitable u's by $v_1, \ldots, v_{s-1}$ generates the same subspace as that generated by the u's and v_s belongs to it; i.e., v_s is linearly dependent on $v_1, \ldots, v_{s-1}$ and certain u's. In expressing that dependence the coefficient of at least one u must be $\neq 0$, since $v_1, \ldots, v_s$ are linearly independent. Thus Theorem 6.2 applies again and we have the desired result. By the method used it is clear that $s \leqslant n$. ■

THEOREM 6.4. If the vector space E over F has a finite basis containing n elements, then every basis of E has n elements.

PROOF: Let $B = \{u_1, \ldots, u_n\}$ and $C = \{y_1, \ldots, y_m\}$ be two bases for E. Since the elements of C generate E and the elements of B are linearly independent, by Theorem 6.3, $n \leqslant m$. Applying the same reasoning with B and C interchanged we have $m \leqslant n$. Therefore, $m = n$. ■

This last theorem justifies the next definition.

DEFINITION 6.1. If the vector space E over the field F has a finite basis, the number of elements in that basis is called the *dimension of E over F*, and is denoted by dim E (unless several fields are involved, then $\dim_F E$).

PROBLEM 6.1. Prove that in a vector space E of dimension n, the elements of any set of $n + 1$ elements of E are linearly dependent.

PROBLEM 6.2. Find a basis for the vector subspace of $V_4(Q)$ generated by $(1,3,5,8)$, $(2,3,7,-1)$, $(8,15,31,13)$.

PROBLEM 6.3. Prove that if a vector space E is of dimension n, then every subspace of E is of dimension $\leqslant n$. (Warning: do not attempt to apply Problem 6.1 immediately. Proceed step by step to find a basis. Then apply Problem 6.1.)

PROBLEM 6.4. Prove that if M is a subspace of the vector space E, then $\dim E = \dim M \Leftrightarrow E = M$.

PROBLEM 6.5. Prove that every set of n linearly independent elements of a vector space E of dimension n is a basis of E.

PROBLEM 6.6. If M, N are subspaces of the vector space E $\ni E = M \oplus N$, prove $\dim E = \dim M + \dim N$. (Hint: take a basis of M and a basis of N and show that the union of these bases is a basis of E.)

PROBLEM 6 7 Prove that if two vector spaces of finite dimension are isomorphic, they have the same dimension (cf Definition 3 4)

PROBLEM 6 8 Prove that if two vector spaces over the same field have the same dimension, they are isomorphic

PROBLEM 6 9 If $E = M + N$, M, N subspaces of the vector space E, prove that $\dim E = \dim M + \dim N - \dim (M \cap N)$

PROBLEM 6 10 Prove that if M is a subspace of E, then $\dim E/M = \dim E - \dim M$

PROBLEM 6 11 Prove that if M is a subspace of the finite dimensional vector space E then $\exists$ a subspace $N \ni E = M \oplus N$ (cf Problem 4 14)

7 MODULES OF LINEAR COMBINATIONS AND LINEAR RELATIONS

First we give a very general definition from the theory of sets

DEFINITION 7 1 If A and B are any two sets then A^B is the set of all mappings of B into A

This is a special case of Definition 4 1 of Chapter 1 in which $I = B$ and $E_\iota = A \quad \forall \iota \in I$

PROBLEM 7 1 Show that our notation R^n used in Section 4 is agreement with this definition

We are interested in the special case of Definition 7 1 in which the set used as a base is a ring (What we do would apply to an additive group but that does not interest us here)

DEFINITION 7 2 Let R be a ring and T any set Then $R^{(T)}$ is the set of all mappings of T into R in which only a finite number of the image elements for a given mapping are different from zero, and for which the following laws of composition hold if a and b are any two such mappings we define their sum $a + b$ by $\iota(a + b) = \iota a + \iota b$, $\forall \iota \in T$ and define an external law between each element $r \in R$ and each mapping a as ra by $\iota(ra) = r(\iota a) \quad \forall \iota \in T$ The mapping a is sometimes given by writing the set of images under a as $(a_\iota)_{\iota \in T}$ and using this notation the two just defined laws of composition may be written as (1) $(a_\iota)_{\iota \in T} + (b_\iota)_{\iota \in T} = (c_\iota)_{\iota \in T}$ where $c_\iota = a_\iota + b_\iota$, and (2) $r(a_\iota)_{\iota \in T} = (ra_\iota)_{\iota \in T}$ and these give us $R_L^{(T)}$ For $R_R^{(T)}$, we use (1) and (2) $r(a_\iota)_{\iota \in T} = (a_\iota r)_{\iota \in T}$ If R is commutative we write merely $R^{(T)}$

THEOREM 7.1. If R has an identity element, then $R_{\mathrm{L}}^{(T)}$ is a unitary left R-module and $R_{\mathrm{R}}^{(T)}$ is a unitary right R-module.

DEFINITION 7.3. Let R be a ring with an identity element, and let $e_\lambda = (a_\iota)_{\iota \in T}$ denote the element of $R^{(T)} \ni a_\lambda = 1$ and $a_\iota = 0$ for $\iota \neq \lambda$. The set of all e_λ, $\lambda \in T$, is called a canonical basis of $R^{(T)}$.

THEOREM 7.2. The e_λ, as defined in Definition 7.3, form a basis of $R^{(T)}$.

PROBLEM 7.2. Prove Theorem 7.1.

PROBLEM 7.3. Prove Theorem 7.2.

PROBLEM 7.4. Explain why in Definition 7.2 the restriction is made that only a finite number of the image elements should be not zero.

PROBLEM 7.5. Relate $R^{(T)}$ with $V_n(R)$.

For any set, T, $t \rightarrow e_t$, $\forall\ t \in T$, is a 1–1 mapping of T onto the set of all e_t. Thus it is merely a change in notation to write t for e_t in expressing elements of $R^{(T)}$. This justifies the following definition.

DEFINITION 7.4. With e_t replaced by t in the expression of any element of the set, the unitary R-module $R^{(T)}$ is called the *module of formal linear combinations* with coefficients in R of elements of T.

PROBLEM 7.6. Write in two ways the general expression for all elements of $Z^{(L)}$ where $L = \{a,f,g,x\}$.

PROBLEM 7.7. Do the same as in Problem 7.6 for $Z^{(M \times N)}$ where $M = \{1,2,3\}$, $N = \{1,2\}$.

THEOREM 7.3. Let $(a_\iota)_{\iota \in T}$ be any nonempty set of elements of a unitary R-module E. The submodule generated by the a_ι is isomorphic to $R_{\mathrm{L}}^{(T)}/N$, where N is the submodule generated by all elements $(x_\iota)_{\iota \in T} \in R_{\mathrm{L}}^{(T)} \ni \Sigma\, x_\iota a_\iota = 0$.

PROBLEM 7.8. Prove Theorem 7.3. [Hint: consider the mapping $(x_\iota) \rightarrow \Sigma\, x_\iota a_\iota$ and apply the generalization of Theorem 4.1 of Chapter 3.]

DEFINITION 7.5. For brevity, the module N of Theorem 7.3 is called the *module of linear relations* between the a_ι.

8. ALGEBRAS

We have thus far considered systems with one, two, and four laws of composition; now we consider one with three.

DEFINITION 8.1 A *ring with operators* is a ring R, a set of elements (called operators) M, and a law of external composition between elements of M and elements of $R \ni$

(1) $\forall\, \alpha \in M \;\; \forall\, x \in R \;\; \alpha x \in R$,

(2) $\forall\, \alpha \in M, \forall\, x, y \in R \;\; \alpha(x+y) = \alpha x + \alpha y$,

(3) $\forall\, \alpha \in M \;\; \forall\, x, y \in R \;\; \alpha(xy) = (\alpha x)y = x(\alpha y)$

As we have done with other systems, we shall usually denote a ring with operators by the letter designating the set of elements.

It should be noted that an operator of a ring with operators does *not* provide an endomorphism of the ring without operators, although it does for the additive group of the ring.

One example of a ring with operators is any ring R with the operators the central of the ring.

Most examples of interest, however, are algebras which we next define.

DEFINITION 8.2 If R is a commutative ring with an identity element, then E is an *algebra over* $R \Leftrightarrow E$ is a ring with operators R and E is a unitary R module with respect to the addition in E.

PROBLEM 8.1 Write out all the conditions relating to the laws of composition in an algebra.

The system defined in Definition 8.2 is sometimes called a *linear associative algebra over R* in contrast to

DEFINITION 8.3 If a set F satisfies all the conditions of an algebra except that multiplication in E is not associative for at least three elements of E, then E is called a (linear) *nonassociative algebra* (or not associative).

EXAMPLE 8.1 (An example of an algebra.) A basis of $V_2(Q)$ is $a = (1, 0)$, $b = (0, 1)$. Let us define the product of these basis elements as follows: $a^2 = a$, $ab = ba = b$, $b^2 = a$. Then a and b and this multiplication form a cyclic group of order 2, and so the associative law holds for these two elements. We shall prove below that if multiplication of basis elements in an R module is associative, then multiplication of any three elements, when defined as one would expect it to be, is associative. (If we had not been able to observe that a and b formed a group, we could always have verified the associative law by considering the eight cases present.) The elements of this algebra are all the expressions of the form $ra + sb$ for $r, s \in Q$. We might ask if there are divisors of zero present. To find out, let us take the product $(r_1a + s_1b)$ $(r_2a + s_2b) = (r_1r_2 + s_1s_2)\, a + (r_1s_2 + r_2s_1)\, b$ and see when it is zero.

It will be zero if $r_1 = \pm s_1$ while $r_2 = \mp s_2$. For example, $(a+b)(a-b) = 0$.

PROBLEM 8.2. Consider the algebra derived from $V_2(Q)$ when multiplication of $a = (1,0)$, $b = (0,1)$ is defined as: $a^2 = a$, $ab = ba = b$, $b^2 = -a$. Show that it is a field.

PROBLEM 8.3. Construct a nonassociative algebra from $V_2(Q)$ by defining products of basis elements suitably.

There are two relatively easy ways (one of which we used above) by which we can construct algebras. One is to take a unitary R-module with a basis and define an associative multiplication for the basis elements. Then by Theorem 8.3 (below), the multiplication is associative for all elements when we define a product of $x = \Sigma_{i=1}^n \xi_i e_i$ and $y = \Sigma_{j=1}^n \eta_j e_j$ as $xy = \Sigma_{i=1}^n (\Sigma_{j=1}^n \xi_i \eta_j e_i e_j)$, where $\{e_i\}$ is the basis. A second way is to take a system such as a group or a semigroup, in which an associative multiplication is already defined and make it into an R-module by taking the set of all formal linear combinations with coefficients in a ring R of the elements of the system. Then, since products of basis elements are already defined, we have merely to define the product of two general elements as above and we have an algebra. In both cases, the distributive law is easy to verify.

PROBLEM 8.4. Show that in the algebras constructed as above, the distributive laws hold.

PROBLEM 8.5. Use the first method to construct an algebra over Z from $V_2(Z)$.

PROBLEM 8.6. Use the second method with the cyclic group of order 3. Is it an integral domain?

PROBLEM 8.7. Do the same as in Problem 8.5 except that in this case make the multiplication of basis elements nonassociative, if possible.

THEOREM 8.1. In an additive abelian group G which is closed with respect to a multiplication (not necessarily associative) and which is distributive with respect to addition,

$$\left(\sum_{i=1}^n r_i\right)\left(\sum_{j=1}^n s_j\right) = \sum_{i=1}^n\left(\sum_{j=1}^n r_i s_j\right) = \sum_{j=1}^n\left(\sum_{i=1}^n r_i\right)s_j, \ \forall\, r_i, s_j \in G.$$

THEOREM 8.2. In a ring,

$$\sum_{i=1}^n a_i\left(\sum_{j=1}^n b_j \sum_{k=1}^n c_k\right) = \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n a_i(b_j c_k), \text{ etc.}$$

PROBLEM 8 8 Verify Theorems 8 1 and 8 2 for the case $n = 2$

PROBLEM 8 9 Prove Theorems 8 1 and 8 2 by induction

THEOREM 8 3 Let E be an R module with a basis $\{a_i\}$ and let multiplication be defined so that E is closed with respect to that multiplication and so that $\forall \alpha \in R$ $\forall \iota$ κ we have $\alpha(a_\iota a_\kappa) = (\alpha a_\iota)a_\kappa = a_\iota(\alpha a_\kappa)$ Then that multiplication is associative $\Leftrightarrow$ the multiplication of basis elements is associative

PROOF Let $x = \Sigma_{i=1}^{n} \xi_i a_i$ $y = \Sigma_{j=1}^{n} \eta_j a_j$ $z = \Sigma_{k=1}^{n} \zeta_k a_k$ be any three elements of E Then $x(yz) = \Sigma \xi_i a_i(\Sigma \eta_j a_j \Sigma \zeta_k a_k) = \Sigma \xi_i a_i (\Sigma \Sigma \eta_j \zeta_k a_j a_k) = \Sigma \Sigma \Sigma \xi_i \eta_j \zeta_k a_i (a_j a_k)$ similarly $(xy)z = \Sigma \Sigma \Sigma \xi_i \eta_j \zeta_k (a_i a_j) a_k$ and from this the result the relation $\Leftarrow$ follows immediately The relation $\Rightarrow$ is obvious ∎

COROLLARY 8 1 The products of the basis elements determine the algebra completely

THEOREM 8 4 If S is an additive semigroup then R_S can be made into an algebra by defining the products of the basis elements as follows e_s $e_t = e_{s+t}$ If S has a neutral element 0 then the algebra derived from R_S has an identity element e_0

PROBLEM 8 10 Find an algebra by using Theorem 8 4

PROBLEM 8 11 Prove Theorem 8 4

9 QUATERNIONS

A very interesting and important algebra over Q can be obtained from $V_4(Q)$ For brevity we introduce letters for the basis elements as follows $e = (1\ 0\ 0\ 0)$ $i = (0\ 1\ 0\ 0)$ $j = (0\ 0\ 1\ 0)$ $k = (0\ 0\ 0\ 1)$ We define multiplication of basis elements as follows $e^2 = e$ $ei = ie = i$ $ej = je = j$ $ek = ke = k$ $ij = -ji = k$ $jk = -kj = i$ $ki = -ik = j$ $i^2 = j^2 = k^2 = -e$

First we note that e is an identity element and so an element of the form qe where $q \in Q$ may be replaced by q Thus any element can be uniquely written in the form $r_0 + r_1 i + r_2 j + r_3 k$ where r_0 r_1 r_2 $r_3 \in Q$

Next we observe that the mapping of the basis elements and their negatives onto the elements of the group Q_8 $1 \leftrightarrow e$ $a \leftrightarrow i$ $b \leftrightarrow j$ $ab \leftrightarrow k$ $b^2 \leftrightarrow -e$ $b^3 \leftrightarrow -j$ $ab^2 \leftrightarrow -i$ $ab^3 \leftrightarrow -k$ is an isomorphism and so the multiplication we have defined for the basis elements is associative

PROBLEM 9.1. Verify that the above mapping is an isomorphism.

DEFINITION 9.1. The algebra defined above is called the *algebra of rational quaternions*. The elements themselves are *rational quaternions*. If $\alpha = a + bi + cj + dk$ is an element of this algebra, $\bar{\alpha} = a - bi - cj - dk$ is called the *conjugate of* α. $\alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$ is called the *norm of* α and is denoted by $N(\alpha)$.

PROBLEM 9.2. Verify the above product of α and $\bar{\alpha}$.

PROBLEM 9.3. Prove that if $\alpha \neq 0$, $\exists\, \alpha^{-1}$, a quaternion, $\ni \alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. (Hint: generalize from the method used in dealing with complex numbers.)

PROBLEM 9.4. Show by an example that an equation of the second degree with rational coefficients can have more than two distinct quaternions as solution. (In fact, infinitely many.)

THEOREM 9.1. The algebra of rational quaternions is a non-commutative division ring.

PROBLEM 9.5. Prove Theorem 9.1.

Chapter 5 Polynomials, Factorization, Ideals, and Extension of Fields

In this chapter we consider several different but related topics First of all we discuss polynomials and polynomial functions defining each carefully and making a careful distinction between them Then we consider some special types of integral domains and factorization in them These we did not consider earlier since many of the best illustrations of them involve polynomials

Next we consider ideals which are for rings to quite an extent what invariant subgroups are for groups By using ideals in polynomial rings over fields we are able to get new fields with certain properties which we desire one of which is that in the new field a polynomial will factor which would not in the original field In order to do this we introduce certain important concepts about fields

Finally we consider the extension of isomorphisms between fields This is of immediate importance in Chapter 6

1 POLYNOMIALS

The reader probably has had some previous experience with polynomials We now define them carefully

Let R be a ring with an identity element and let I be the set of nonnegative rational integers By Theorem 7 1 of Chapter 4 $R_L{}^I$ is a unitary left R module which we shall denote briefly by R The set of the e_λ $\lambda \in I$ as defined in Definition 7 3 of Chapter 4 form a basis of R Since I is an additive semigroup we can define an associative multiplication of the e_λ by e_s $e = e_s$ From this relation it follows immediately by induction that $e_n = e$ $\forall n \in Z^*$ If we denote e by x we have $e_n = x$ $\forall n \in Z^*$ Thus we now have a basis for R consisting of e_0 x x^2 and furthermore $e_0 x^n = x^n e_0 = x^n$ Lastly since the set of all elements re_0 $\forall r \in R$ is a ring isomorphic to R and since $re_0 x = rx$ we may replace re_0 by r e_0 by 1 the identity element of R If we now consider the module of all linear combinations of $e_0, x, x^2, \ldots$ and define products as follows: if $u = \sum_{i=0}^{n} \xi_i x^i$, $v = \sum_{j=0}^{n} \eta_j x^j$, then $uv = \sum_{i=0}^{n} \sum_{j=0}^{n} \xi_i \eta_j x^{i+j}$, $\alpha u = \sum_{i=0}^{n} (\alpha \xi_i) x^i$, $\forall\ \alpha \in R$, and we have, by applying Theorem 8.3 of Chapter 4, defined a ring which we shall denote by $R[x]$. (For x^0, see Definition 15.1 of Chapter 2.) If R is commutative, then $R[x]$ is an algebra over R.

Definition 1.1. The ring $R[x]$, is called the *polynomial ring* in x over R, and if R is commutative, the *polynomial algebra* in x over R. An element, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i \in R[x]$ is called a *polynomial* in the *indeterminate* x, the a_i are called the *coefficients* of $f(x)$, a_i is called the *coefficient of* x^i; and if one or more of the a_i are $\neq 0$, then the smallest integer n satisfying $a_i = 0$, $\forall\ i > n$, (such an integer exists by Definition 7.2 of Chapter 4) is called the *degree* of $f(x)$, (often denoted by *deg f*), with a_n the *leading coefficient*. A polynomial whose leading coefficient is 1 is called *monic*. If all $a_i = 0$, the polynomial is called the *zero polynomial* and does not have a degree.

It should be noted that the original ring R is imbedded in $R[x]$. Sometimes it is convenient to use some letter other than x as the indeterminate. If we wish to define $R[y]$, for example, we need merely go back in the above discussion and call e_1, y.

Sometimes the degree of the zero polynomial is taken to be $-\infty$ with the understanding that $-\infty < a$ for each nonnegative a. This has some advantages, such as in Theorem 1.4 below it is unnecessary to give the alternatives $r_1(x) = 0$ and $r_2(x) = 0$, and also in Theorem 4.1 below, if we agree that $2^{-\infty} = 0$, it is unnecessary to give the additional condition that $\delta(0) = 0$.

Theorem 1.1. Let S be a subring of a ring R with an identity element. Then the set of all linear combinations of $1, x, x^2, \ldots$, with coefficients in S is a subring of $R[x]$, and will be denoted by $S[x]$.

Proof: Apply Theorem 5.1 of Chapter 4. ■

In the above theorem, the ring S need not have an identity. This enables us to consider polynomials over rings without identities since any ring S can be imbedded in a ring with an identity element. This was established in Problem 1.23 of Chapter 4 although late in this chapter we shall obtain a better result.

Problem 1.1. Using in turn each of the two forms for the basis elements, find the sum and product of the following polynomials, their degrees, and the degrees of the sum and product, as elements of $Z[x]$:

$(3, 4, -2, 0, 0, \ldots)$, $(1, 2, 3, 0, 0, \ldots)$. ('$\ldots$' here means that all following coefficients are zero.)

Problem 1.2 Do the same as in Problem 1.1 for the following elements of $Z_6[x]$. (a) $(1, 3, 5, 0, 0, \ldots)$, $(3, -5, 0, 0, \ldots)$. (b) $(4, 3, 0, 0, \ldots)$, $(-2, 3, 0, 0, \ldots)$.

Theorem 1.2 $f(x) = \Sigma_{i=0}^{n} a_i x^i$ and $g(x) = \Sigma_{i=0}^{m} b_i x^i \in R[x]$ $\Rightarrow f(x)g(x) = \Sigma_{i=0}^{n+m} c_i x^i$, where $c_i = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$.

Theorem 1.3 $f(x)$, $g(x) \in R[x]$, $f(x) + g(x) = h(x)$, $f(x)g(x) = k(x) \Rightarrow \deg k \leqslant \deg f + \deg g$, $\deg h \leqslant \max(\deg f, \deg g)$, if h and k have degrees.

Corollary 1.1 If R has no divisors of zero, then $\deg k = \deg f + \deg g$.

Corollary 1.2 If R is an integral domain, then $R[x]$ is an integral domain.

Problem 1.3 Prove Theorem 1.2 (by induction).

Problem 1.4 Prove Theorem 1.3.

Problem 1.5 Give three examples in which the strict inequalities hold in Theorem 1.3.

Problem 1.6 Prove Corollaries 1.1 and 1.2.

Problem 1.7 Prove that the leading coefficient of $f(x)$ is regular, $g(x) \neq 0 \Rightarrow \deg f(x)g(x) = \deg f(x) + \deg g(x)$.

The reader should observe a number of similarities between polynomial rings and Z. The next theorem is like Theorem 17.1 of Chapter 2.

Theorem 1.4 (Division Algorithm.) Let R be a ring with an identity element and let $a(x)$, $b(x) \in R[x]$. Further, let $\deg b(x) = n \geqslant 0$ and let b_n be a unit of R. Then $\exists\, q_1(x)$, $r_1(x)$, $q_2(x)$, $r_2(x) \in R[x] \ni a(x) = b(x)q_1(x) + r_1(x)$, $a(x) = q_2(x)b(x) + r_2(x)$ where $r_1(x) = 0$ or $\deg r_1(x) < \deg b(x)$ and $r_2(x) = 0$ or $\deg r_2(x) < \deg b(x)$. Finally, the $q_i(x)$ and $r_i(x)$, $i = 1, 2$, are unique.

Proof We shall prove the existence of $q_1(x)$ and $r_1(x)$ and leave the rest to the reader.

If $a(x) = 0$, then the theorem holds with $q_1(x) = r_1(x) = 0$.

The proof of the theorem is immediate if $\deg a(x) < \deg b(x)$, for then we take $q(x) = 0$ and $r(x) = a(x)$. So we shall suppose that $\deg a(x) \geqslant \deg b(x)$.

If $a(x) = a_0$, then we can take $q_1(x) = b_0^{-1}a_0$, $r_1(x) = 0$.

Now let deg $a(x) = 1$; then $a(x) = a_1x + a_0$ and $b(x) = b_1x + b_0$, since deg $b(x)$ is 1 or 0. If $b_1 = 0$, take $q_1(x) = b_0^{-1}a(x)$, $r_1(x) = 0$; if $b_1 \neq 0$, take $q_1(x) = b_1^{-1}a_1$; $r_1(x) = a_0 - b_0b_1^{-1}$. Thus the theorem holds if deg $a(x) = 1$.

Now suppose that the theorem holds for all $a(x)$ of degree $\leqslant n$, and let $a(x) = a_{n+1}x^{n+1} + a_nx^n + \cdots + a_0$, $b(x) = b_mx^m + \cdots + b_0$, where b_m has an inverse in R. We may suppose, by an earlier remark, that $m \leqslant n + 1$. Consider $h(x) = a(x) - b(x)b_m^{-1}a_{n+1}x^{n+1-m}$. Then $h(x)$ is of degree n at most, and so by induction hypothesis $\exists\ \overline{q_1(x)}$ and $\overline{r_1(x)} \ni h(x) = b(x)\overline{q_1(x)} + \overline{r_1(x)}$, where $\overline{r_1(x)} = 0$ or deg $\overline{r_1(x)}$ $<$ deg $b(x)$. Then $a(x) = b(x)[b_m^{-1}a_{n+1}x^{n+m} + \overline{q_1(x)}] + \overline{r_1(x)} = b(x)$ $q_1(x) + r_1(x)$, where $q_1(x) = b_m^{-1}a_{n+1}x^{n+m} + \overline{q_1(x)}$, $r_1(x) = \overline{r_1(x)}$ and $r_1(x) = 0$ or deg $r_1(x) <$ deg $b(x)$.

Therefore, the theorem follows by induction. We leave the proof of the uniqueness as an exercise. ■

Corollary 1.3. If, in Theorem 1.4, R is a field, q_1, q_2, r_1, r_2 always exist if $b(x) \neq 0$, and $q_1 = q_2$, $r_1 = r_2$.

Problem 1.8. Prove the uniqueness (use Problem 1.7).

Problem 1.9. Prove Theorem 1.4 for $q_2(x)$, $r_2(x)$ including uniqueness.

Problem 1.10. Find $q(x)$, $r(x)$ if $a(x) = x^4 + 2x^3 - 3x^2 + 5x + 1$, $b(x) = x^3 - 2x + 2$, $R = Q$.

Problem 1.11. Do Problem 1.10 with $R = Z_7$.

Problem 1.12. Do Problem 1.10 with $R = Z_6$.

Problem 1.13. For $a(x) = x^4 + (-3i + 2k)x^3 + (2 + 3i)x^2 + (9 - i + 4k)x + (6i + 3k)$, $b(x) = x^2 - 3ix + (2 - j)$, where the coefficients are rational quaternions, find $q_1(x)$, $r_1(x)$ and $q_2(x)$, $r_2(x)$.

Problem 1.14. Prove that Theorem 1.4 applies to $Z[x]$ with conclusion that $Na(x) = b(x)q(x) + r(x)$, where $N \in Z$. Can this be generalized to any arbitrary ring?

2. POLYNOMIALS AND POLYNOMIAL FUNCTIONS

It is important to realize that a polynomial and a polynomial function, which we are about to define, are quite different. This section is devoted principally to considering the relations between them.

Definition 2.1 Let $f(x) = \sum_{i=1}^{n} a_i x^i \in R[x]$, and let $c \in R$. First, $f_R(c) = \sum_{i=0}^{n} a_i c^i$, $f_L(c) = \sum_{i=0}^{n} c^i a_i$. Secondly, the mapping $c \rightarrow f_R(c)$ $(c \rightarrow f_L(c))$ of R into R is called the *right (left) polynomial function* determined by the polynomial $f(x)$. If R is commutative, these two functions coincide and the mapping is called the polynomial function determined by $f(x)$. In this case since no confusion can result we usually denote the function by $f(x)$.

The above is not completely standardized and some authors interchange the definitions of $f_R(c)$ and $f_L(c)$.

Problem 2.1 Show that in general the above mapping $c \rightarrow f(c)$ is not a homomorphism of R.

Problem 2.2 For $f(x) = x^3 + (i - j)x^2 + kx + 2i$ where the coefficients are rational quaternions find $f_L(j)$, $f_R(j)$.

Problem 2.3 For $f(x) = i + jx$, $g(x) = j - kx$ find $h(x) = f(x)g(x)$. Then show that $f_R(j)g_R(j) \neq h_R(j)$.

The property displayed in Problem 2.3 that $f_R(c)g_R(c) \neq h_R(c)$ when $h(x) = f(x)g(x)$ is illustrative of the difficulties which may arise if R is not commutative. However we can establish one useful result in case $f_L(c) = 0$ or $g_R(c) = 0$. For this we need the following

Lemma $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i \in R[x] \Rightarrow h(x) = f(x)g(x) = \sum_{i=0}^{n} a_i(\sum_{j=0}^{m} b_j x^j)x^i = \sum_{j=0}^{m} x^j(\sum_{i=0}^{n} x^i a_i)b_j$.

Theorem 2.1 Let R be a ring with an identity element, let $c \in R$, $f(x)$, $g(x) \in R[x]$ and let $h(x) = f(x)g(x)$. Then $g_R(c) = 0 \Rightarrow h_R(c) = 0$, $f_L(c) = 0 \Rightarrow h_L(c) = 0$.

Proof By the above lemma $h_R(c) = \sum_{i=0}^{n} a_i(g_R(c))c^i = 0$, $h_L(c) = \sum_{j=0}^{m} c^j f_L(c) b_j = 0$. ■

Problem 2.4 Prove the lemma.

Problem 2.5 Consider the statement of Theorem 2.1 for $g_L(c) = 0$ and for $f_R(c) = 0$.

Problem 2.6 Prove that R is commutative, $c \in R$, $h(x) = f(x)g(x) \Rightarrow h(c) = f(c)g(c)$.

Problem 2.7 Verify Theorem 2.1 for the polynomial functions of Problem 2.3 using $c = i$.

Theorem 2.2 (The Remainder Theorem) In applying Theorem 1.4 to $a(x) \in R[x]$ and $b(x) = x - c$ where $c \in R$ we have $r_1(x) = a_L(c)$ and $r_2(x) = a_R(c)$.

PROOF: Since deg $(x - c) = 1$, we have $r_i(x) = 0$ or deg $r_i(x) = 0$. Hence, $r_i(x) \in R$ for $i = 1, 2$. The rest follows by applying Theorem 2.1 with $g(x) = x - c$ and then with $f(x) = x - c$. ■

PROBLEM 2.8. Apply Theorem 2.2 to the polynomial of Problem 2.2.

DEFINITION 2.2. Let $f(x) \in R[x]$ and let S be a ring containing R as a subring. Then $c \in S$ is a *right (left) zero* of $f(x) \Leftrightarrow f_R(c) = 0$ $(f_L(c) = 0)$. If S is commutative, we say merely a *zero* of $f(x)$.

THEOREM 2.3. Let $f(x) \in I[x]$, where I is an integral domain. Then $c \in I$ is a zero of $f(x) \Rightarrow x - c | f(x)$.

DEFINITION 2.3. Let $f(x) \in I[x]$, where I is an integral domain. Then $a \in I$ is a zero of $f(x)$ of *multiplicity* (sometimes called *order*) $m \Leftrightarrow (x - a)^m | f(x)$ while $(x - a)^{m+1} \nmid f(x)$.

THEOREM 2.4. $f(x) \in I[x]$, where I is an integral domain $\Rightarrow$ $f(x)$ has at most n zeros if deg $f(x) = n \geqslant 0$.

It is important to observe that two different polynomials may determine the same polynomial function. For example, let $f(x) = x^3 + 2x^2 + x$ and $g(x) = x^7 + 2x^6 + x^5$, considered as elements of $Z_5[x]$. Then the two polynomials are, of course, different, while the functions determined by them are the same since $f(0) = 0 = g(0)$, $f(1) = 4 = g(1)$, $f(2) = 3 = g(2)$, $f(3) = 3 = g(3)$, $f(4) = 0 = g(4)$. The next theorem gives a condition sufficient to insure that this cannot happen.

THEOREM 2.5. If $f(x)$, $g(x) \in I[x]$, where I is an integral domain with infinitely many elements, then if the polynomial functions determined by $f(x)$ and $g(x)$ are equal for all $x \in I$, the polynomials $f(x)$ and $g(x)$ are equal.

COROLLARY 2.1. Under the conditions of Theorem 2.5, if $f(x)$ and $g(x)$ are equal for $n + 1$ elements where deg $f \leqslant n$, deg $g \leqslant n$, then $f = g$.

PROBLEM 2.9. Prove Theorems 2.3, 2.4, 2.5 and Corollary 2.1.

DEFINITION 2.4. If $f(x) = \Sigma_{i=0}{}^n a_i x^i \in R[x]$, then the *derivative* of $f(x)$ is $f'(x) = \Sigma_{i=1}^n i a_i x^{i-1}$.

THEOREM 2.6. $f(x), g(x) \in R[x] \Rightarrow (f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$, $(f(x) + g(x))' = f'(x) + g'(x)$, $(f(g(x)))' = f'(g(x)) g'(x)$, and deg $f'(x) <$ deg $f(x)$, if deg $f(x) > 0$ and if $f'(x)$ has a degree. [If $f(x)$ is given as in Definition 2.4, $f(g(x)) = \Sigma_{i=0}^n a_i (g(x))^i$.]

Problem 2 10 Prove Theorem 2 6 (use only Definition 2 4)

Problem 2 11 Find a field F and a polynomial $f(x) \in F[x]$ $\ni \deg f'(x) < [\deg f(x) - 1]$

Theorem 2 7 Let $f(x) \in I[x]$, $c \in I$, an integral domain The element c is a zero of $f(x)$ of multiplicity $m > 1 \Rightarrow x - c | f\ (x)$

Proof Let c be a zero of order m Then by Definition 2 3 and Definition 16 1 of Chapter 2, $f(x) = (x - c)^m \phi(x)$, where $\phi(x) \in I[x]$, and by Theorem 2 3 and Definition 2 3, $\phi(c) \neq 0$ Then by Theorem 2 6 and Definition 2 4, $f\ (x) = m(x - c)^{m-1}\phi(x) + (x - c)^m \phi\ (x) = (x - c)^{m-1}[m\phi(x) + (x - c)\phi'(x)]$, which, since $m > 1$, $\Rightarrow$ $(x - c)^{m-1} | f\ (x) \Rightarrow (x - c) | f\ (x)$ ∎

Corollary 2 2 If c is a zero of multiplicity m of $f(x)$, then c is a zero of multiplicity at least $m - 1$ of $f\ (x)$

Problem 2 12 Apply Theorem 2 6 to find the multiple zero of $f(x) = x^3 - 3x^2 + 3x - 1$

Problem 2 13 Find an example of a polynomial such that the words at least in the above corollary are necessary (Hint use Problem 2 11)

3 GAUSSIAN SEMIGROUPS AND GAUSSIAN DOMAINS

We are now going to consider various factorization theorems first in a general semigroup customarily with multiplication as the law of composition as in Definitions 16 1 through 16 8 of Chapter 2 then in particular for certain types of rings One extremely important property possessed by many rings (Z is one such) is that of having a unique (or essentially unique) factorization for each nonzero nonunit element into a product of irreducible elements and intimately connected with this is the property of an irreducible element being a prime One simple example of a ring in which unique factorization does not hold is $R[x]$ where R is the division ring of rational quaternions here we have $x^2 + 1 = (x - i)(x + i) = (x - j)(x + j) = (x - k)(x + k)$, and in each case the factors are obviously irreducible since they are of the first degree Of course, in this case the ring is not commutative However it is possible to give an example in a commutative ring in which factorization is not unique

Theorem 3 1 If S is a commutative semigroup with a neutral element and in which the cancellation law holds for every element, then $p \in S$, p is a prime $\Rightarrow p$ is irreducible

Proof: Let $p = ab, a, b \in S$. Then by Definition 16.6 of Chapter 2, since $ab = 1 \cdot p$, either $p|a$ or $p|b$. Suppose for definiteness that $p|a$. Then $a = pc, c \in S$. So $p = pcb \Rightarrow 1 = cb \Rightarrow c$, b are units and so, since b is a unit (by Definition 16.5 of Chapter 2), p is irreducible. ■

In general, the converse of this theorem is not true. We have already given an example of a noncommutative ring in which the converse is not true, since $(x - i) \neq (x - j)$, etc.

Definition 3.1. A commutative multiplicative semigroup S with a neutral element and in which the cancellation law holds for each element is called *Gaussian* ⇔ every nonunit in S has an essentially unique factorization (cf. Definition 18.1 of Chapter 2) as a product of irreducible elements.

In a Gaussian semigroup the converse of Theorem 3.1 does hold.

Theorem 3.2. S is a Gaussian semigroup, $p \in S$, p irreducible $\Rightarrow p$ is prime.

Proof: Let $p|ab$, where $a, b \in S$. Then $\exists\, c \in S \ni ab = pc$. Now $c = e_c \Pi\, p_\iota$, where e_c is a unit of S, and p_ι is irreducible for each ι. Also $a = e_a \Pi\, q_\iota$, $b = e_b \Pi\, r_\iota$, where e_a, e_b are units in S and q_ι, r_ι are irreducible. Therefore, $e_a e_b \Pi\, q_\iota \Pi\, r_\iota = pe_c \Pi\, p_\iota$ and so, since S is Gaussian, p is an associate of some q_i or some r_ι. In the former case, $p|a$, and in the latter, $p|b$. Therefore, p is a prime. ■

Theorem 3.3. S is a Gaussian semigroup, $a, b \in S \Rightarrow a$ and b have a greatest common divisor.

Corollary 3.1. Any finite number of elements in a Gaussian semigroup have a greatest common divisor.

Problem 3.1. Prove Theorem 3.4.

Problem 3.2. Prove Corollary 3.1.

Problem 3.3. Prove that in $F[x]$, where F is a field, all irreducible elements are polynomials of degree $n \geqslant 1$. (Hint: show all nonzero elements of F are units.)

Definition 3.2. $f(x) \in A[x], f(x) \neq 0$, A is a Gaussian domain. Then $f(x)$ is *primitive* ⇔ every g.c.d. of the coefficients of $f(x)$ is a unit.

Theorem 3.4. Let A be a Gaussian domain, and F its field of quotients (cf. Definition 1.8 of Chapter 4). Let $f_1(x), f_2(x) \in A[x]$

be primitive Then $f_1(x), f_2(x)$ are associates in $F[x] \Leftrightarrow f_1(x), f_2(x)$ are associates in $A[x]$

Proof Since $f_1(x)$ $f_2(x)$ are associates in $F[x]$, $\exists\, \alpha \neq 0$, $\alpha \in F$ $\ni f_1(x) = \alpha f_2(x)$ Then $\alpha = d_2 d_1^{-1}$, where $d_1, d_2 \in A$ Then $d_1 f_1(x) = d_2 f_2(x)$ Thus d_1 divides all the coefficients of $d_2 f_2(x)$ and so since $f_2(x)$ is primitive $d_1 | d_2$ Similarly, $d_2 | d_1$ Therefore, $d_2 = d_1 e$, where e is a unit in A Therefore, $f_1(x) = e f_2(x)$ Therefore $f_1(x)$, $f_2(x)$ are associates in $A[x]$ ∎

Theorem 3 5 (Gauss Lemma) $f(x)$, $g(x) \in A[x]$, A is Gaussian $f(x)$ $g(x)$ are primitive $\Rightarrow f(x)g(x)$ is primitive

Proof Let $f(x) = \sum_{i=0}^{n} a_i x^i$ $g(x) = \sum_{i=0}^{m} b_i x^i$, $f(x)g(x) = \sum_{i=0}^{n+m} c_i x^i$ and suppose that $f(x)g(x)$ is not primitive Then $\exists\, p \in A$, p irreducible $\ni p | c_i$ $i = 0, 1, \ldots, n + m$ Since $f(x)$ is primitive not all a_i are divisible by p Let a_k be the first of the a_i not divisible by p and similarly let b_j be the first b_i not divisible by p Now the coefficient of x^{k+j} is $a_k b_j + a_{k+1} b_{j-1} + \cdots + a_{k-1} b_{j+1} + \cdots$ Here p divides all terms except the one written first and so since by hypothesis $p | c_{k+j}$ $p | a_k b_j$ Hence by Theorem 3 2 $p | a_k$ or $p | b_j$ which is a contradiction Therefore $f(x)g(x)$ is primitive ∎

Theorem 3 6 $f(x) \in A[x]$ A is Gaussian $f(x)$ is irreducible in $A[x]$ $\deg f(x) > 0 \Rightarrow f(x)$ is irreducible in $F[x]$ where F is the field of quotients of A

Problem 3 4 Prove Theorem 3 7 [Hint suppose $f(x) = \phi_1(x)\phi_2(x)$ in $F[x]$ Then find common denominators for the coefficients of $\phi_1(x)$ and $\phi_2(x)$]

Theorem 3 7 (Eisenstein) Let $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ where A is Gaussian and $f(x)$ is primitive If $\exists$ a prime $p \in A \ni p | a_i$ $\forall\, i < n$ $p \nmid a_n$ $p^2 \nmid a_0$ then $f(x)$ is irreducible in $A[x]$

Problem 3 5 Prove Theorem 3 8 [Hint assume a factorization of $f(x)$ and proceed in a manner similar to the proof of Theorem 3 6]

Problem 3 6 If $f(x) = \sum_{i=0}^{n} a_i x^i$ we define $f(x + c)$ as the polynomial obtained by expanding $\sum_{i=0} a_i (x + c)^i$ Now prove that if I is an integral domain then $f(x) \in I[x]$ is irreducible in $I[x] \Leftrightarrow f(x + c)$ is irreducible in $I[x]$

Problem 3 7 Prove that the cyclotomic polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x - 1)$ p a positive rational prime is irreducible in $Z[x]$ (Hint replace x by $x + 1$ then use Problem 3 6)

Problem 3.8. Prove that if I is an integral domain, $c, r \in I$, $c|r$, then $c|r^n$, $\forall\, n \in Z^*$.

Problem 3.9. Prove that if I is an integral domain, p a prime in I, $p|r^n$, then $p|r$.

Problem 3.10. Prove that if A is a Gaussian domain, a, b, $c \in A$, a and c are relatively prime, $c|ab$, then $c|b$.

Theorem 3.8. Let A be a Gaussian domain and let F be its field of quotients. Let $f(x) \in A[x]$, $r/s \in F$, r, s be relatively prime, and $f(r/s) = 0$. Then, if $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a primitive polynomial, $s|a_n$ and $r|a_0$.

Corollary 3.2. If a_n is a unit in A, then all the zeros of $f(x)$ in R are in A.

Problem 3.11. Prove Theorem 3.8 and its corollary.

Problem 3.12. Prove that the following polynomials are irreducible in $Z[x]$: (a) $x^2 - 3$, (b) $x^2 + x + 3$, (c) $x^3 - 2$, (d) $x^3 - x + 2$. (Hint: if a polynomial of degree 2 or 3 is reducible, it must have a linear factor.)

Problem 3.13. Give an example of a reducible polynomial of degree 4 or higher, reducible in $Z[x]$, but having no linear factor in $Z[x]$.

Problem 3.14. Prove that if p is a prime in Z, $\nexists\, a \in Q \ni a^n = p$, for $n > 1, n \in N$.

Problem 3.15. Generalize the statement of Problem 3.14.

Problem 3.16. Prove that the following polynomials are reducible in $Z[x]$: (a) $x^4 + 2x^2 + 1$, (b) $x^4 + x^2 + 1$.

Problem 3.17. Find all irreducible polynomials of degree 2 in $Z_2[x]$; find some such of degree 3.

Problem 3.18. Do the same as in Problem 3.17 for $Z_3[x]$.

4. EUCLIDEAN DOMAINS

We now consider a type of domain which we shall presently prove is Gaussian.

Definition 4.1. An integral domain I is a *Euclidean domain* $\Leftrightarrow \exists$ a mapping δ of I into the nonnegative integers such that (1) $\delta(a)$

$= 0 \Leftrightarrow a = 0$ (2) $\forall\, a\ b \in I$ $\delta(ab) = \delta(a)\delta(b)$ (3) $\forall\, a\ b \in I$ $b \neq 0$ $\exists\, q\ r \in I \ni a = bq + r$ where $\delta(r) < \delta(b)$

THEOREM 4 1 The following are Euclidean domains

(1) Z with $\delta(a) = |a|$

(2) $F[x]$ where F is a field with $\delta(f(x)) = 2^{\deg f(x)}$ if $f(x) \neq 0$ $\delta(0) = 0$

PROOF Theorem 17 1 of Chapter 2 Theorem 1 3 of this chapter and its corollary ■

THEOREM 4 2 Let $a \in I$ a Euclidean domain Then $\delta(a) = 1$ $\Leftrightarrow a$ is a unit of I

PROOF First we note that $\delta(1) = 1$ since $1 = 1 \cdot 1$ and so by (2) of Definition 4 1 $\delta(1) = \delta(1)\delta(1)$ and since $\delta(1) \in Z^*$ $\delta(1) = 1$

Consider the implication $\Leftarrow$ Let a be a unit Then $\exists\, b \in I \ni ab = 1$ So $\delta(a)\delta(b) = 1$ and since $\delta(a) \in Z^*$ $\delta(a) = 1$

Consider now the implication $\Rightarrow$ Let $\delta(a) = 1$ Then $\exists\, q\ r \in I$ $\ni 1 = aq + r$ with $\delta(r) < \delta(a) = 1 \Rightarrow \delta(r) = 0 \Rightarrow 1 = aq \Rightarrow a$ is a unit ■

THEOREM 4 3 $a\ p \in I$ a commutative ring with an identity element p irreducible $\Rightarrow$ a g c d of a and p is an associate of 1 or of p

THEOREM 4 4 $p \in I$ a Euclidean domain p irreducible $\Rightarrow p$ is prime

THEOREM 4 5 A Euclidean domain is Gaussian

PROBLEM 4 1 Prove Theorem 4 3

PROBLEM 4 2 Prove Theorem 4 4 (Follow the proof of Theorem 17 6 of Chapter 2)

PROBLEM 4 3 Prove Theorem 4 5 (Follow the proof of Theorem 17 7 of Chapter 2)

PROBLEM 4 4 Prove that if $f(x)\ g(x) \in F[x]$ F a field $\exists$ $s(x)\ t(x) \in F[x] \ni s(x)f(x) + t(x)g(x) = d(x)$ where $d(x)$ is the monic g c d of $f(x)$ and $g(x)$

THEOREM 4 6 A is a Gaussian domain $\Rightarrow A[x]$ is a Gaussain domain

PROBLEM 4 5 Prove Theorem 4 6 (Hint let F be the field of quotients of A Then apply Theorems 4 1 4 5 3 7 etc)

5. POLYNOMIALS IN TWO INDETERMINATES

Let R be a ring with an identity element and, as before, let I be the set of nonnegative integers. Then by Theorem 7.1 of Chapter 4, $R^{(I\times I)}$ is a left R-module having as basis $\{e_{m,n}\}$ where $e_{m,n} = (b_{i,j}{}^{m,n})_{(i,j)\in I\times I}$, where $b_{m,n}{}^{m,n} = 1$ and $b_{i,j}{}^{m,n} = 0$ for $(m, n) \neq (i,j)$. We define $e_{r,s} \cdot e_{u,v} = e_{r+u,s+t}$. Then $e_{0,0}$ is a neutral element for multiplication and if we let $e_{1,0} = x$, $e_{0,1} = y$, we have $e_{m,n} = x^m y^n$ for $(m, n) \in I \times I$. Then, as before, by Theorem 8.3 of Chapter 4, we have an associative multiplication defined in $R^{(I\times I)}$ and it is distributive with respect to addition when we make the usual definition of the product of two elements when expressed as a linear combination of the basis elements. Lastly, we replace the element $re_{0,0}$ by r, $\forall\, r \in R$.

DEFINITION 5.1. The ring defined above is called the *ring of polynomials in the two indeterminates* x, y and is denoted by $R[x, y]$, and if R is commutative, it is called a *polynomial algebra*. An element $f(x, y) = \Sigma_{i=0}^{m} \Sigma_{j=0}^{n} a_{ij}x^i y^j \in R[x, y]$, is called a *polynomial in the indeterminates* x, y, the a_{ij} are called the *coefficients* of $f(x, y)$, a_{ij} is called the *coefficient of* $x^i y^j$, and if one or more of the $a_{ij} \neq 0$, and if a_{mn} is a coefficient such that $m + n$ is maximum of $i + j$ for all nonzero a_{ij}, then $m + n$ is the *degree* of $f(x, y)$.

To consider such a ring as $(R[x])[y]$ is possible following a remark in Section 1, but it is notationally simpler to call the elements of the basis over $R[x]$ $f_0, f_1, f_2, \ldots$ and in particular f_1, y. Using this and the above definition the following theorem may easily be proved.

THEOREM 5.1. If R is a commutative ring with an identity element, the following rings are isomorphic: $R[x, y]$, $(R[x])[y]$, $R[y, x]$, $(R[y])[x]$.

PROBLEM 5.1. Prove Theorem 5.1.

PROBLEM 5.2. Examine the theorems pertaining to $R[x]$ and see which ones generalize to $R[x, y]$.

6. FIELDS OF QUOTIENTS OF POLYNOMIALS

DEFINITION 6.1. If F is a field, the field of quotients of $F[x]$ is denoted by $F(x)$; that of $F[x, y]$ by $F(x, y)$. [*Note:* elements of the above fields are sometimes called rational functions of x or of x and y.]

THEOREM 6.1. If I is an integral domain, and F its field of quotients, then the field of quotients of $I[x]$ is $F(x)$, that of $I[x, y]$ is $F(x, y)$.

PROBLEM 6.1. Prove Theorem 6.1.

7. IDEALS

We are now going to consider a particular kind of subring which for rings plays much the same role as does an invariant subgroup for groups.

DEFINITION 7.1. A subring $\mathfrak{a}$ of a ring R is a *left (right) ideal* $\Leftrightarrow$ $\mathfrak{a}$ is a left (right) R module. A *two sided* (also called *bilateral*) *ideal* is a subring which is both a left and a right ideal in R.

If it is clear from the context, or if it does not matter (as is the case if R is commutative) which side an ideal is, we shall say merely ideal.

PROBLEM 7.1. Prove that $\mathfrak{a}$ is a left (right) ideal in a ring $R \Leftrightarrow$ (1) $\mathfrak{a}$ is a subring of R and (2) $\forall a \in \mathfrak{a}, \forall r \in R, ra \in \mathfrak{a}$ $(ar \in \mathfrak{a})$.

PROBLEM 7.2. Prove that $\mathfrak{a}$ is a left (right) ideal in a ring $R \Leftrightarrow$ (1) $\forall a_1, a_2 \in \mathfrak{a}, a_1 - a_2 \in \mathfrak{a}$ and (2) $\forall a \in \mathfrak{a}, \forall r \in R, ra \in \mathfrak{a}$ $(ar \in \mathfrak{a})$.

PROBLEM 7.3. Prove that in Z the multiples of an integer m form an ideal.

PROBLEM 7.4. Prove that in $F[x]$, where F is a field, the multiples of any particular polynomial $f(x)$ form an ideal.

PROBLEM 7.5. Prove that in $F[x, y]$, where F is a field, the set of all polynomials with $a_{00} = 0$ form an ideal.

PROBLEM 7.6. Prove that in every ring (except one ring) there are at least two distinct ideals.

PROBLEM 7.7. Determine all the ideals in a division ring, in a field.

THEOREM 7.1. *Let S be a set of ideals in a ring R. Then the common part of the ideals of S is an ideal in R and is contained in every ideal of S.*

THEOREM 7.2. *Let $\mathfrak{a}$ be an ideal in a ring R. Then, considering R as an R module, $\mathfrak{a}$ is a submodule of R. Further, if A is any set of elements of R, the smallest left (right) ideal in R containing A*

is the submodule generated by A (cf. Definition 5.2 of Chapter 4). This ideal is called the *left (right) ideal generated by* A.

Problem 7.8. Prove Theorems 7.1, and 7.2.

Problem 7.9. Let $A \subset R$, a ring. Give the general form of an element in the left ideal generated by A.

Problem 7.10. Do the same as in Problem 7.9 for a ring with an identity element.

Problem 7.11. Give an example of a ring and an ideal in it for which the form of Problem 7.10 is necessary.

Definition 7.2. An ideal $\mathfrak{M}$ is a *principal ideal* $\Leftrightarrow$ $\mathfrak{M}$ is generated by a single element a. If a principal ideal is bilateral, it is usually denoted by (a).

Problem 7.12. Show that the ideals of Problems 7.3, 7.4 are principal ideals.

Problem 7.13. Show that the ideal of Problem 7.5 is not a principal ideal.

Problem 7.14. Give the form of a general element of a principal ideal in a ring when R has an identity element and when R does not.

Problem 7.15. Prove that if R has an identity element, then $R = (1)$.

8. PRINCIPAL IDEAL RINGS

Definition 8.1. A ring R is a *principal ideal ring* $\Leftrightarrow$ every ideal in R is principal.

Theorem 8.1. A Euclidean domain is a principal ideal ring.

Corollary 8.1. Z and $F[x]$, where F is a field, are principal ideal rings.

Problem 8.1. Prove Theorem 8.1 and its corollary.

Problem 8.2. Show that a Gaussian domain need not be a principal ideal ring. (Hint: use Theorem 4.6 twice and Problems 7.5, 7.13.)

Theorem 8.2. An integral domain I is a principal ideal ring $\Leftrightarrow$

(1) $\forall a, b \in I$, a, b not both zero, $\exists$ a g.c.d. d of a and b, $d \in I$

(2) $\exists r, s \in I \ni d = ra + sb$

(3) if in the sequence $a_1, a_2, a_3, \ldots$ of elements of I each is a divisor of the preceding, $\exists n \ni \forall k \geqslant n$, a_k is an associate of a_n.

PROBLEM 8.3 Prove Theorem 8.2.

9. QUOTIENT RINGS AND EQUIVALENCE RELATIONS IN A RING

In Chapter 3, we found in Theorems 3.1 and 3.2 a complete solution to the problem of determining which equivalence relations were compatible with the structure of a group. Here, we consider the same problem for rings. The complete solution is given by Theorems 9.1 and 9.2. As promised, ideals play the role which invariant subgroups played before.

DEFINITION 9.1 An equivalence relation P defined between elements of a ring R is *compatible with the structure of R* (or sometimes more briefly, with R) $\Leftrightarrow P$ is compatible with all internal and external laws of composition of R.

THEOREM 9.1 If $\mathscr{M}$ is a bilateral ideal in a ring R, then the relation $(xPy \Leftrightarrow x - y \in \mathscr{M})$ is an equivalence relation compatible with R.

PROBLEM 9.1 Prove Theorem 9.1. (Hint: use Theorem 3.1 of Chapter 3 and Definition 7.1.)

THEOREM 9.2 Every equivalence relation P in a ring R compatible with R is of the form $(xPy \Leftrightarrow x - y \in \mathscr{M})$, where $\mathscr{M}$ is a bilateral ideal of R.

PROBLEM 9.2 Prove Theorem 9.2. (Hint: use Theorem 3.2 of Chapter 3.)

THEOREM 9.3 Let R be a ring, $\mathscr{M}$ a bilateral ideal in R, P the equivalence relation of Theorem 9.1. Then the quotient set of R by P is a ring.

PROOF This follows immediately from Theorems 12.1, 12.2, 12.4 of Chapter 2 and Theorem 3.8 of Chapter 3 generalized to groups with operators. ∎

DEFINITION 9.2 The ring whose existence is established by Theorem 9.3 is denoted by $R/\mathscr{M}$ and is called the *quotient ring of R* *with respect to* $\mathcal{M}$. Sometimes it is called a *difference ring* and is denoted by $R - \mathcal{M}$. The equivalence relation of Theorem 9.3 is often denoted by $x \equiv y \bmod \mathcal{M}$.

Problem 9.3. Prove that in Z, $a \equiv b \bmod (m)$ is equivalent to $a \equiv b \bmod m$. Thus show that $Z/(m)$ is isomorphic to Z_m.

Problem 9.4. Let R be the ring of even integers and $\mathcal{M} = (6)$. Find $R/\mathcal{M}$.

Problem 9.5. Let $R = Z_{24}$, $\mathcal{M} = (3)$, $\mathcal{B} = (6)$. Find $Z_{24}/\mathcal{M}$ and $Z_{24}/\mathcal{B}$. Are there divisors of zero in either of these rings?

Problem 9.6. Let $R = Z_2[x]$, $\mathcal{M} = (x^2 + x + 1)$. Find $R/\mathcal{M}$. Letting θ represent the equivalence class containing x, write the addition and multiplication tables for $R/\mathcal{M}$. Is it a field?

Problem 9.7. Do the same as in Problem 9.6 for $R/\mathcal{M}$ where $\mathcal{M} = (x^3 + x + 1)$.

In stating the next theorem, we write the letter for a homomorphism as an exponent. We shall frequently do this in Chapter 6.

Theorem 9.4. Let α be a homomorphism of a ring R into a ring S. Then the set of all elements $r \in R \ni r\alpha = 0$ is a bilateral ideal $\mathcal{M}$ in R and $R\alpha$ is isomorphic to $R/\mathcal{M}$.

Problem 9.8. Prove Theorem 9.4.

10. PRIME AND MAXIMAL IDEALS

Definition 10.1. An ideal $\mathcal{M}$ in a ring R, *is a prime ideal in* $R \Leftrightarrow (ab \in \mathcal{M}, a, b \in R \Rightarrow \text{either } a \in \mathcal{M} \text{ or } b \in \mathcal{M})$.

Definition 10.2. An ideal $\mathcal{M} \neq R$ in a ring R, is a *maximal (divisorless)* ideal $\Leftrightarrow$ ($\mathcal{B}$, an ideal in R, $\mathcal{B} \neq \mathcal{M}$, $\mathcal{B} \supset \mathcal{M} \Rightarrow \mathcal{B} = R$).

Problem 10.1. Prove that in Z, if p is a prime, (p) is prime and maximal.

Problem 10.2. Prove that if $\phi(x)$ is irreducible in $F[x]$, where F is a field, then $(\phi(x))$ is prime and maximal.

Problem 10.3. In $I[x, y]$, where I is a Gaussian domain in which 2 is a prime, show that the following ideals are prime: (x), (x, y), $(x, y, 2)$, and show that $(x, y, 2)$ is maximal.

Problem 10.4. Show that the ideal of Problem 7.5 is a maximal ideal.

In Problem 10 3 we have two examples of prime ideals which are not maximal However in a commutative ring with an identity element every maximal ideal is prime See Corollary 10 1 below

The nature of the quotient ring $R/\mathfrak{m}$ naturally depends in part on the nature of the ring R but also on the nature of the ideal $\mathfrak{m}$ For example R may have no divisors of zero while $R/\mathfrak{m}$ does [for instance $Z/(6)$] or on the other hand R may have divisors of zero and lack an identity element while $R/\mathfrak{m}$ may be a field The next two theorems give important information in this respect

THEOREM 10 1 Let R be a commutative ring with an identity element and $\mathfrak{m}$ an ideal in R Then $R/\mathfrak{m}$ is an integral domain $\Leftrightarrow \mathfrak{m}$ is a prime ideal

PROOF Let $\mathfrak{m}$ be a prime ideal Using the notation introduced in Definition 9 2 to show that $R/\mathfrak{m}$ is an integral domain we must show that if $ab = 0 \bmod \mathfrak{m}$ $a \not\equiv 0 \bmod \mathfrak{m}$ then $b \equiv 0 \bmod \mathfrak{m}$ But this follows immediately from the definition of prime ideal since $x = 0 \bmod \mathfrak{m} \Leftrightarrow x \in \mathfrak{m}$

Let $R/\mathfrak{m}$ be an integral domain We must show that if $ab \in \mathfrak{m}$ then either $a \in \mathfrak{m}$ or $b \in \mathfrak{m}$ Suppose that $a \notin \mathfrak{m}$ Then $a \not\equiv 0 \bmod \mathfrak{m}$ Thus if $ab \in \mathfrak{m}$ $ab = 0 \bmod \mathfrak{m}$ and since an integral domain does not have divisors of zero we must have $b = 0 \bmod \mathfrak{m} \Rightarrow b \in \mathfrak{m}$ Therefore $\mathfrak{m}$ is prime ∎

THEOREM 10 2 Let R be a commutative ring with an identity element and $\mathfrak{m}$ an ideal in R Then $R/\mathfrak{m}$ is a field $\Leftrightarrow \mathfrak{m}$ is a maximal ideal

PROOF Let $\mathfrak{m}$ be a maximal ideal To show that $R/\mathfrak{m}$ is a field it is sufficient to show that each equivalence class not zero has an inverse For this it is sufficient to show that for any $c \in R \ni c \not\equiv 0 \bmod \mathfrak{m}$ $\exists\, b \in R \ni cb = 1 \bmod \mathfrak{m}$ Then the equivalence class containing b will be the inverse of that containing c Consider the ideal generated by $\mathfrak{m}$ and c Since $\mathfrak{m}$ is a maximal ideal and $c \notin \mathfrak{m}$ this ideal is $R = (1)$ i e 1 is in the ideal generated by $\mathfrak{m}$ and c Thus $\exists\, a \in \mathfrak{m}$ and $b \in R \ni 1 = a + b$ Therefore $1 = bc \bmod \mathfrak{m}$ Therefore $R/\mathfrak{m}$ is a field

Let $R/\mathfrak{m}$ be a field Then given $c \not\equiv 0 \bmod \mathfrak{m}$ $\exists\, b \in R \ni cb = 1 \bmod \mathfrak{m}$ This implies that the ideal generated by $\mathfrak{m}$ and any element $\notin \mathfrak{m}$ contains 1 and is therefore the whole ring R Therefore $\mathfrak{m}$ is maximal ∎

COROLLARY 10 1 Under the conditions of Theorem 10 1 or 10 2 a maximal ideal is prime

PROBLEM 10.5. Prove Corollary 10.1 without using Theorem 10.2.

PROBLEM 10.6. Let R be a commutative ring without divisors of zero and let W be the ring obtained in Problem 1.23 of Chapter 4. Let Y be the set of all $z \in W \ni \forall\, r \in R$, $zr = 0$. Prove that Y is a prime ideal in W.

PROBLEM 10.7. Let R be a commutative ring without divisors of zero. Prove that $\exists$ an integral domain D containing R as a subring. (Hint: let $D = W/Y$ where W and Y are as in Problem 10.6.) This is the improvement on Problem 1.23 of Chapter 4 which was promised earlier.

11. EXTENSIONS OF FIELDS

In the rest of this chapter we are going to consider fields. First, we shall prove in this section that certain types of extensions of fields exist, then we shall analyze the structure of fields. Finally, we shall at the end of the chapter consider extensions of isomorphisms between fields.

THEOREM 11.1. Let F be a field. There always exists a field K containing F as a subfield and an element $\theta \in K$ such that θ is not a zero of any polynomial of positive degree $f(x) \in F[x]$.

PROOF: One such field is $F(x)$, the field of quotients of $F[x]$, as defined in Definition 6.1. One such element θ can be taken to be x, since if it were the zero of a polynomial $f(x) \in F[x]$, we would have the elements $1, x, x^2, \ldots, x^n$ linearly dependent, where $n = \deg f(x)$, and this is impossible since $1, x, x^2, \ldots$ form a basis of $F[x]$ and so are linearly independent over F. ∎

THEOREM 11.2. Let F be a field. If $\exists$ a polynomial $f(x) \in F[x] \ni$

(1) $\deg f \geq 2$,

(2) $f(x)$ is irreducible in $F[x]$, then $\exists$ a field K containing F as a subfield $\ni K$ has a zero θ of $f(x)$. (Here we use "containing" in the sense that F is imbedded in K, as we have been doing.)

PROOF: By Problem 10.2, $(f(x))$ is a maximal ideal in $F[x]$. Hence by Theorem 10.2, $F[x]/(f(x))$ is a field. The equivalence classes of K determined by elements of F form a field isomorphic to F, and the equivalence class determined by x is a zero of $f(x)$. ∎

EXAMPLE 11.1. $f(x) = x^2 + x + 1$ is an irreducible polynomial in $Z_2[x]$, and so by Theorem 10.2 $Z_2[x]/(x^2+x+1)$ is a field K. We wish to determine the elements of this field. By Theorem 1.4 every polynomial $g(x) \in Z_2[x]$ is $g(x) \equiv ax+b \bmod (x^2+x+1)$ where $a, b \in Z_2$. Thus there are only four equivalence classes in K. Let the equivalence class containing x be θ and those determined by 0, 1 be denoted by 0, 1 respectively. Then the four elements of K are 0, 1, θ, $\theta+1$. Since θ is a zero of x^2+x+1 we have $\theta^2+\theta+1=0$ or $\theta^2=\theta+1$ and by this last relation we can determine all products. Thus $\theta \cdot (\theta+1)=\theta^2+\theta=\theta+1+\theta=1$, $(\theta+1)^2=\theta^2+1=\theta+1+1=\theta$, etc.

Example 11.2 $f(x)=x^3-2$ is an irreducible polynomial in $Q[x]$ and so $Q[x]/(x^3-2)$ is a field K. We wish to determine the elements of this field. By Theorem 1.4 if $g(x) \in Q[x]$, $g(x) \equiv ax^2+bx+c \bmod (x^3-2)$ and here we have infinitely many elements in K since there are infinitely many choices for a, b, c. Let θ denote the equivalence class containing x and let the equivalence class determined by $r \in Q$ be denoted by r. Then since θ is a zero of x^3-2 we have $\theta^3=2$. Thus $(\theta^2+2)(\theta^2-5\theta+1)=\theta^4-5\theta^3+3\theta^2-10\theta+2=2\theta-10+3\theta^2-10\theta+2=3\theta^2-8\theta-8$. If it is desired to find the inverse of $c_2\theta^2+c_1\theta+c_0$ then one way is to use Problem 4.4 with $f(x)=x^3-2$ and $g(x)=c_2x^2+c_1x+c_0$. Then $(c_2\theta^2+c_1\theta+c_0)^{-1}=t(\theta)$.

Problem 11.1 Prove the last statement above.

Problem 11.2 For the field of Example 11.2 find $(\theta^2-4\theta+1)^{-1}$.

Problem 11.3 Take any polynomial you found in Problem 3.18 which is irreducible in $Z_3[x]$ and describe the field obtained by using it as in Example 11.1.

Problem 11.4 Prove that $f(x)=x^3+x+1$ is irreducible in $Q[x]$ and discuss the field obtained by using it as was done in Example 11.2 with x^3-2.

Problem 11.5 Describe the field $Q[x]/(x^4-2)$. Find the inverse of θ^2+3 in it, where θ is the zero obtained for x^4-2.

12 STRUCTURE OF FIELDS

Theorem 12.1 Let K be a field containing F as a subfield. Then K is a vector space over F.

Proof This follows directly from Problem 4.4 of Chapter 4 since K is a K module. ∎

Note: Henceforth, for brevity, if we write the field $K \supset F$, we shall mean that the field K contains the field F as a subfield, unless some remark is made specifically to the contrary.

DEFINITION 12.1. Let $K \supset F$. Then the dimension of K over F is called the *degree of K over F* and is denoted by $[K:F]$, if it is finite.

THEOREM 12.2. Let $K \supset F$ and let $\theta \in K$. The vector space L over F generated by $1, \theta, \theta^2, \ldots$, i.e., the set of all θ^i, $i \in \{0\} \cup N$, is a subintegral domain I of K and is the smallest integral domain in K containing F and θ.

PROOF: The element 1 is an identity element, there are no divisors of zero since we are dealing with a field K, and closure with respect to multiplication follows from the obvious fact that the product of two elements of the form $\Sigma a_i\theta^i$ is another element of the same form. ■

DEFINITION 12.2. Let $K \supset F, \theta \in K$. Then θ is *algebraic* or *transcendental over F* according as the integral domain I of Theorem 12.1 as a vector space over F has finite dimension or not.

THEOREM 12.3. Let $K \supset F, \theta \in K$, and θ be algebraic over F. Then

(1) $\exists$ a unique monic polynomial $f(x) \in F[x]$, irreducible in $F[x] \ni f(\theta) = 0$

(2) the dimension of I, of Theorem 12.2 for θ, is equal to the degree of $f(x)$,

(3) for θ, the integral domain of Theorem 12.2 is a field, the smallest subfield of K which contains F and θ.

PROOF: Let n be the dimension of I over F. Then by Problem 6.1 of Chapter 4, the elements $1, \theta, \theta^2, \ldots, \theta^n$ are linearly dependent over F; i.e., $\exists\, a_0, a_1, \ldots, a_n \in F$, not all zero, $\ni a_0 + a_1\theta + a_2\theta^2 + \cdots + a_n\theta^n = 0$. Then $a_n \neq 0$, for otherwise, if a_j were the particular a_i of largest subscript of the nonzero a_i, then we should have on dividing by a_j, $\theta^j = b_0 + b_1\theta + \cdots + b_{j-1}\theta^{j-1}, j < n$, from which it follows immediately that a subset of $1, \theta, \ldots, \theta^{j-1}$ (perhaps the whole set) would form a basis of I, and I would not be of dimension n over F. So, if we let $c_i = a_i/a_n$, we have θ a zero of the monic polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in F[x]$, and we have proved that θ cannot be a zero of a polynomial of lower degree.

We must show that $f(x)$ is irreducible in $F[x]$. Suppose, on the contrary, that $f(x) = g(x)h(x)$, where $g(x), h(x) \in F[x]$ and each is of positive degree Then $f(\theta) = g(\theta)h(\theta)$ and since K is a field either $g(\theta) = 0$ or $h(\theta) = 0$ But by the above this is impossible since $g(x)$ and $h(x)$ are by hypothesis of degree less than n

We must show that $f(x)$ is unique Let $g(x) \in F[x]$ be monic and $g(\theta) = 0$ Clearly $\deg g \geq n$ Hence by Theorem 1 4 $\exists\ q(x)$ $r(x) \in F[x] \ni g(x) = f(x)q(x) + r(x)$ and $r(x) = 0$ or $\deg r(x) < n$ Now $0 = g(\theta) = f(\theta)q(\theta) + r(\theta) \Rightarrow r(\theta) = 0 \Rightarrow r(x) = 0$ since otherwise $0 \leq \deg r(x) < n$ Therefore $g(x) = f(x)q(x)$ and if $g(x)$ is irreducible in $F[x]$ $\deg q(x) = 0$ and if $g(x)$ is monic $q(x) = 1$ and $f(x) = g(x)$

We have now established conclusions (1) and (2) To prove (3) we first show that each nonzero element of I has an inverse in I Let $\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \in I$ Let $g(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ Since $f(x)$ is irreducible $(f(x)\ g(x)) = 1$ and so by Problem 4 4 $\exists\ s(x)\ t(x) \in F[x] \ni s(x)f(x) + t(x)g(x) = 1$ Then since $f(\theta) = 0$ we have $t(\theta)g(\theta) = t(\theta)\alpha = 1$ i e $t(\theta)$ is the inverse of $g(\theta)$ and $t(\theta) \in I$ Since any subfield of K containing F and θ must contain I all is proved ∎

DEFINITION 12 3 Let $K \supset F$ $\theta \in K$ θ algebraic over F Then if $f(x)$ is the irreducible monic polynomial in $F[x]$ having θ as a zero $f(x)$ is called the *minimum polynomial of θ over F* and the degree of $f(x)$ is the *degree of θ over F*

DEFINITION 12 4 Let $K \supset F$ and $\theta \in K$

(1) if θ is algebraic over F the integral domain I of Theorem 12 2 which in this case is a field is denoted by $F(\theta)$

(2) if θ is transcendental over F the field of quotients of the integral domain of Theorem 12 2 is denoted by $F(\theta)$

(3) let $K \supset L \supset F$ Then L is a *simple extension of F* $\Leftrightarrow \exists\ \theta \in L \ni L = F(\theta)$

(4) K is *algebraic over F* $\Leftrightarrow$ each element of K is algebraic over F Otherwise K is *transcendental over F*

COROLLARY 12 1 Every element of $F(\theta)$ if θ is algebraic over F can be expressed uniquely in the form $d_0 + d_1\theta + \cdots + d_{n-1}\theta^{n-1}$ where $d_i \in F$ $i = 0\ 1 \ldots n-1$ and where n is the degree of θ over F

COROLLARY 12 2 The degree of θ over F if θ is algebraic over F is equal to the degree of $F(\theta)$ over F

COROLLARY 12 3 If $f(x)$ is the minimum polynomial of θ algebraic over F and if $g(\theta) = 0$ $f(x) \in F[x]$ then $f(x) \mid g(x)$

THEOREM 12.4. Let F be a field. Then there always exists a field K which is a transcendental extension of F.

PROOF: The field of quotients of the polynomial ring over F is such a field. ■

LEMMA. Let $K \supset F$ and $\theta \in K$. Then $\theta \in F \Leftrightarrow$ the minimum polynomial of θ over F is of the first degree.

PROBLEM 12.1. Prove the lemma.

With the above lemma and Theorem 12.3, we can restate Theorem 11.2 as follows:

THEOREM 12.5. Let F be a field. Then $\exists$ an element θ, algebraic over F and a simple extension, $F(\theta) \neq F$, of $F \Leftrightarrow \exists\, f(x) \in F[x]$ of degree $n \geqslant 2 \ni f(x)$ is irreducible in $F[x]$. In the latter case, $F(\theta)$ has a zero of $f(x)$.

PROBLEM 12.2. Finish the proof of Theorem 12.5.

THEOREM 12 6. Let $L = F(\theta)$ be a simple extension of a field F, let θ be algebraic over F, and let $\phi \in L$. Then ϕ is algebraic over F, and the degree of ϕ over F is $\leqslant$ degree of θ over F.

PROOF: By Theorem 12.3 and Definition 12.3, the degree n of θ is equal to the degree of $F(\theta)$, i.e., is equal to the dimension of $F(\theta)$ as a vector space over F. Since $\phi \in F(\theta)$, ϕ is equal to a linear combination with coefficients in F of $1, \theta, \theta^2, \ldots, \theta^{n-1}$ and hence so is every power of ϕ. Thus the set $1, \phi, \phi^2, \ldots, \phi^n$ are $n+1$ elements of the vector space $F(\theta)$ and so are linearly dependent. Thus by Definition 12.2, ϕ is algebraic over F, and since $F(\phi) \subset F(\theta)$, degree of $\phi \leqslant n$. ■

COROLLARY 12.4. Let $\theta \in K \supset F$. If θ is algebraic over F, $F(\theta)$ is algebraic over F.

PROBLEM 12.3. For the field of Example 11.2, find the degree of $\theta + 1$; of θ^2; of $\theta^2 + 1$.

PROBLEM 12.4. For the field $Q(\theta)$ of Problem 11.5, find the degree of θ^2, its minimum polynomial, and describe the field $L = Q(\theta^2)$. Find the degree of θ over L and describe $L(\theta)$. Do the same for θ^3 over Q and $M = Q(\theta^3)$.

PROBLEM 12.5. Consider $g(x) = x^6 - 2 \in Q[x]$ and the field $Q[x]/(g(x))$. Treat this as in Problem 12.4. Describe the fields $Q(\theta^2)$, $Q(\theta^3)$, $Q(\theta^4)$, $Q(\theta^5)$.

Problem 12 6 Let $F = Z_p(t)$ where p is a prime and t is transcendental over Z_p Show that $f(x) - x^p - 1$ is irreducible in $F[x]$ (Hint use Theorem 3 8 with A of the theorem $Z_p[t]$) Let θ be a zero of $f(x)$ Show that θ is a zero of multiplicity p of $f(x)$ and show that $F(\theta) - F(\theta)$ for $i - 1$ $p - 1$

13 ADJUNCTION OF SEVERAL ELEMENTS TO A FIELO

We call the process of proceeding from a field F to a field K containing F and one or more specified elements adjunction of those elements to the field F

Definition 13 1 Let $K \supset F$ and let A be any set of elements of K Then $F(A)$ is the smallest subfield of K which contains F and all the elements of A

That such a field always exists follows by considering the common part of all subfields of K which contain F and A

Theorem 13 1 Let $K \supset F$ and θ_1 $\theta_2 \in K$ Then $(F(\theta))(\theta_2) - (F(\theta_2))(\theta_1) = F(A)$ where $A - \{\theta_1$ $\theta_2\}$

Problem 13 1 Prove Theorem 13 1

Problem 13 2 Generalize Theorem 13 1 to the adjunction of θ_1 θ_n Use induction to prove it

Theorem 13 2 Let $K \supset L \supset F$ Then if $[K \; F]$ is finite $[K \; F] = [K \; L]$ $[L \; F]$

Proof Let $[L \; F] = n$ and $[K \; L] - m$ and let β_1 β_n be a basis of L over F α_1 α_m be a basis of K over L We shall show that the mn elements $\alpha_1\beta_1$ $\alpha_1\beta_2$ $\alpha_1\beta_n$ $\alpha_2\beta_1$ $\alpha_2\beta_2$ $\alpha_m\beta_n$ form a basis of K over F

First let $x \in K$ Then $x - \Sigma_i^m{}_1 d \alpha_i$ where the $d \in L$ and so $d_i - \Sigma_{j=1}^n e_{ij}\beta_j$ where the $e_{ij} \in F$ Then $x = \Sigma_i^m{}_1 \Sigma_{j=1}^n e_{ij}\alpha \beta_j$ where the $e_{ij} \in F$ Hence every element of K can be expressed as a linear combination of these mn elements with coefficients in F

Now we must show the linear independence of these mn elements Suppose $\Sigma_{=1}^m \Sigma_{j=1}^n c_{ij}\alpha_i\beta_j = 0$ where the $c_{ij} \in F$ Then rewriting the equation as $\Sigma_{i=1}^m (\Sigma_{j=1}^n c_{ij}\beta_j)\alpha = 0$ we have $\Sigma_{j=1}^n c_{ij}\beta_j = 0$ for $i = 1$ 2 m since $\Sigma_{j=1}^m c_{ij}\beta_j \in L$ and the α form a basis of K over L But since the β_j are linearly independent over F we have $c_{ij} - 0$ for $i = 1$ 2 m $j = 1$ 2 n Therefore $\alpha_1\beta_1$ $\alpha_1\beta_2$ $\alpha_m\beta_n$ form a basis of K over R and the theorem follows ■

COROLLARY 13.1. Let $K \supset L \supset F$, $K \supset H \supset F$, $M = L(H)$. Then $[M:F] \leqslant [L:F] \cdot [H:F]$.

COROLLARY 13.2. If θ is of degree n over F and ϕ is of degree m over F, then $F(\theta, \phi)$ is of degree $\leqslant mn$ over F.

COROLLARY 13.3. If θ is of degree n over F and ϕ is of degree m over $F(\theta)$, then $F(\theta, \phi)$ is of degree mn over F.

THEOREM 13.3. If the field K is of degree n over the field F, and if $\theta \in K$ and θ is of degree m over F, then $m|n$.

COROLLARY 13.4. If $\phi \in F(\theta)$, where θ is algebraic of degree n over F, then ϕ is algebraic over F, and the degree of ϕ over F divides the degree of θ over F.

PROBLEM 13.3. Prove the corollaries to Theorem 13.2.

PROBLEM 13.4. Prove Theorem 13.3 and its corollary.

PROBLEM 13.5. Let $f(x) = x^3 - 2$ and $g(x) = x^2 - 5$ be elements of $Q[x]$. Let θ be a zero of $f(x)$ and ϕ be a zero of $g(x)$. Show: (a) $f(x)$ is irreducible in $Q(\phi)[x]$. [Hint: take a general element of $Q(\phi)$ and show that it cannot be a zero of $f(x)$.] (b) $g(x)$ is irreducible in $Q(\theta)[x]$, (c) $(Q(\phi))(\theta) = (Q(\theta))(\phi)$ and this field is of degree 6 over Q.

PROBLEM 13.6. (a) Let θ be a zero of $f(x) = x^3 - 2 \in Q[x]$. Show that in $Q(\theta)[x]$, $f(x) = (x - \theta)(x^2 + \theta x + \theta^2)$.

(b) Let $g(x) = x^2 + x + 1$. Show that $g(x)$ is irreducible in $Q(\theta)[x]$. (Hint: use Corollary 13.4.)

(c) Let ω be a zero of $g(x)$. Show that $f(\omega\theta) = f(\omega^2\theta) = 0$ and so $Q(\omega, \theta)$ contains all the zeros of $f(x)$.

(d) Show that the degree of $Q(\omega, \theta)$ over Q is 6.

THEOREM 13.4. Let $f(x) \in F[x]$, where F is a field. Then $\exists$ a field $K \supset F \ni$ in $K[x]$, $f(x)$ factors into a product of factors of the first degree $\in K[x]$.

PROBLEM 13.7. Prove Theorem 13.4 by repeated application of Theorem 11.2.

DEFINITION 13.2. Let $f(x) \in F[x]$, where F is a field.

(1) if $f(x)$ is irreducible in $F[x]$, a smallest field K containing F and θ, a zero of $f(x)$, is called a *stem field of $f(x)$ over F*,

(2) a smallest field L containing F and all the zeros of $f(x)$ [i.e., a smallest field $L \ni$ in $L[x]$, $f(x)$ factors as in Theorem 13.4. We shall often describe this by saying that $f(x)$ *factors completely*] is

called a *splitting field of* $f(x)$ *over* F (older terminology was *root field*) It should be noted that in part (2) we do not require that $f(x)$ be irreducible in $F[x]$

PROBLEM 13 8 Prove that $Q(\omega\ \theta)$ of Problem 13 6 is a splitting field of x^3-2 over A and show that $Q(\theta)$ $Q(\omega\ \theta)$ $A(\omega^2\ \theta)$ are stem fields

PROBLEM 13 9 Show that $Q(\omega\ \theta)$ is a splitting field of x^3-2 over $Q(\theta)$ and give the stem fields of x^3-2 over $Q(\omega)$

PROBLEM 13 10 Give stem fields and a splitting field of x^4-2 over Q

PROBLEM 13 11 Do the same as in Problem 13 10 for x^2-2 over Q

PROBLEM 13 12 Do the same as in the last problem for the $f(x)$ of Example 11 1

PROBLEM 13 13 Find an irreducible polynomial of degree three of $Z_2[x]$ and find its stem fields and splitting field over Z_2

14 TRISECTION OF AN ARBITRARY ANGLE

For this we need the following three exercises the first two of which are useful for other purposes as well

PROBLEM 14 1 Let $f(x\ y)$ $g(x\ y) \in F[x\ y]$ where F is a field be of degree 1 Defining a solution of $h(x\ y)=0$ for any $h(x\ y) \in F[x\ y]$ is an ordered pair $(a\ b) \in K \times K$ where $K \supset F \ni h(a\ b)=0$ show that the solutions common to $f(x\ y)=0$ and $g(x\ y)=0$ are in $F \times F$

PROBLEM 14 2 Let $f(x\ y)$ $g(x\ y) \in F[x\ y]$ where F is a field be of degree 1 or be of the form $(x-a)^2+(y-b)^2-r^2$ where $a\ b\ r \in F$ then the solutions common to $f(x\ y)=0$ and $g(x\ y)=0$ $\in K \times K$ where K is of degree 1 or 2 over F

PROBLEM 14 3 Prove that $4x^3$ $3x-t$ is irreducible in $Q(t)$ $[x]$ where t is transcendental over Q (Hint use Theorem 3 8 with $A=Q[t]$)

By the use of straightedge and compasses all lengths which can be constructed by Problems 14 1 2 3 are of degree 2 over A (The identity of Q is the unit of length) Since for an arbitrary angle θ a line-segment of length $\cos\theta$ can be constructed, if it were possible to trisect θ, it would be possible to construct a line-segment of length $\cos(\theta/3)$. Now $4\cos^3(\theta/3) - 3\cos(\theta/3) = \cos\theta$ (verify), so if it were possible to trisect θ, it would be possible to construct a line-segment which was a zero of $4x^3 - 3x - t$, where $t = \cos\theta$. Let $\theta = 60°$. Then since this polynomial is irreducible in $Q[x]$ (verify), any zero would be of degree 3 over Q. But this could not belong to a field of constructible elements by Corollary 13.4, since $3 \nmid 2^n$ for any $n \in N$. Thus an angle of 60° cannot be trisected in the prescribed manner. Similar reasoning applies to many other angles.

Problem 14.4. Fill in the details of the above discussion.

15. EXTENSIONS OF ISOMORPHISMS

We are now going to consider the following situation: $\exists$ an isomorphism α between two fields, $F, \bar{F}$; K and $\bar{K}$ are extensions of $F, \bar{F}$, respectively. Now we ask, when can the isomorphism α be extended to an isomorphism between K and $\bar{K}$? Definition 3.4 of Chapter 1 is the definition of an extension of a mapping and so is pertinent here. We shall here, as will be customary in the following chapter, write the symbol for an isomorphism as an exponent.

Theorem 15.1. Let $R, \bar{R}$ be two isomorphic commutative rings with identity elements and let α be an isomorphism between them. Then $\exists$ an isomorphism β between $R[x]$ and $\bar{R}[x] \ni \alpha$ is the restriction of β to R. Further, $f(x) \in R[x]$ is irreducible in $R[x]$ $\Leftrightarrow$ $[f(x)]^\beta$ is irreducible in $\bar{R}[x]$.

Problem 15.1. Prove Theorem 15.1. (Hint: define β as follows: $\forall\, r \in R$, $r^\beta = r^\alpha$, $x^\beta = x$, etc.)

Theorem 15.2. Let $F, \bar{F}$ be two isomorphic fields under the isomorphism α. Let $f(x) = f_0 + f_1x + \cdots + f_nx^n$ be irreducible in $F[x]$ and let $\bar{f}(x) = [f(x)]^\beta = \bar{f}_0 + \bar{f}_1x + \cdots + \bar{f}_nx^n$, where $\bar{f}_i = f_i^\alpha$, and where β is the extension of α of Theorem 15.1. Then, if θ is a zero of $f(x)$ and $\bar{\theta}$ is a zero of $\bar{f}(x)$, α can be extended to an isomorphism γ of $F(\bar{\theta})$ onto $\bar{F}(\theta) \ni \theta^\gamma = \theta$.

Proof: $F(\theta)$ is isomorphic to $F[x]/(f(x))$ and $\bar{F}(\bar{\theta})$ is isomorphic to $\bar{F}[x]/(\bar{f}(x))$. The isomorphism β of Theorem 15.1 thus induces an isomorphism γ between these two quotient rings and clearly if $a \in F$, $\bar{a} = a^\alpha \in \bar{F}$, then the image under γ of the equivalence class determined by a is the equivalence class determined by a^α. ∎

THEOREM 15.3. Let $f(x)$ be irreducible in $F[x]$, where F is a field. Then

(1) all stem fields of $f(x)$ over F are isomorphic.

(2) all splitting fields of $f(x)$ over F are isomorphic.

PROBLEM 15.2. Verify Theorem 15.3 for the stem fields in Problems 13.8 and 13.10.

PROBLEM 15.3. Determine which of the fields in Problem 12.5 are stem fields. Why are not all $Q(\theta^i)$ isomorphic?

PROBLEM 15.4. Prove Theorem 15.3 by repeated application of Theorem 15.2.

DEFINITION 15.1. Let F, L_1, L_2, K be fields $\ni F \subset L_1 \subset K$ and $F \subset L_2 \subset K$. Then L_1 and L_2 are *conjugate subfields* of K over $F \Leftrightarrow \exists$ an automorphism α of $K \ni$ (1) $L_1^\alpha = L_2$ and (2) $x^\alpha = x$ $\forall x \in F$.

PROBLEM 15.5. Let $f(x)$ be irreducible in $F[x]$ and K the splitting field of $f(x)$ over F. Prove that the stem fields of $f(x)$ over F are conjugate subfields of K over F.

Chapter 6: Fields

The simplest fields which we have considered are the field of rational numbers and the fields consisting of the residue classes modulo p, where p is a prime. It is proved in Section 1 that every field has a subfield isomorphic to exactly one of these. So in many discussions it is necessary to bear this in mind and to distinguish between them. We do so.

Approximately the first two thirds of the chapter is devoted to introducing concepts about fields, to proving results involving them, and to proving the fundamental results of the Galois Theory of Fields.

The last third of the chapter is devoted to the Galois Theory of Equations and to a consideration of the possibility of finding a general formula for the roots of an equation of degree n in terms of the coefficients and addition, subtraction, multiplication, division, and the extraction of roots.

1. PRIME FIELDS

In Chapter 4, the characteristic of a ring was defined. We now prove a result about the characteristic of any integral domain and so of any field.

THEOREM 1.1. An integral domain I has characteristic $p > 0$ $\Rightarrow p$ is a prime in Z.

PROOF: Suppose that p is not a prime. Then $p = m \cdot n$, where $m > 1, n > 1$. Then by the definition of characteristic and by Problem 1.12 of Chapter 4, $m \cdot 1 \neq 0, n \cdot 1 \neq 0$, but $(m \cdot 1)(n \cdot 1) = p \cdot 1 = 0$ and so $\exists$ divisors of zero. This is impossible. Therefore, p is prime. ■

COROLLARY 1.1. The characteristic of a division ring is either zero or a rational prime.

DEFINITION 1.1. The smallest subfield of a field F is called the *prime subfield* of F. A field which has no proper subfields is called a *prime field.*

THEOREM 1 2 A field F has exactly one prime subfield

PROOF The common part of all subfields of F is a subfield of F with the desired properties ∎

The next two theorems characterize completely prime subfields and prime fields

THEOREM 1 3 If a field F has characteristic zero its prime subfield is isomorphic to Q the field of rational numbers

PROOF Now $1 \in F$ and so do n 1 $(-n)$ 1 $(m-n)$ 1 $\forall$ m $n \in Z$ Therefore F contains a subring I generated by 1 and isomorphic to Z Therefore since F is a field it must contain the field of quotients of I say Π which is isomorphic to Q ∎

COROLLARY 1 2 A prime field of characteristic zero is isomorphic to Q

THEOREM 1 4 If a field F has characteristic $p > 0$ its prime subfield Π is isomorphic to $Z_p - Z/(p)$

PROOF Now $1 \in \Pi$ and so do 0 1 1 2 1 $(p-1)$ 1 and since $(m \quad 1)(n \quad 1) = r \quad 1$ where $mn = r \bmod p$ $0 \leqslant r < p$ these p elements form a ring isomorphic to Z_p which is a field ∎

COROLLARY 1 3 A prime field of characteristic $p > 0$ is isomorphic to Z_p

PROBLEM 1 1 Find the prime subfields of all fields so far considered

PROBLEM 1 2 Prove that if F is a field of characteristic $p > 0$ then $\forall$ a $b \in F$ and $\forall f \in Z^*$ (a) $(a+b)^p - a^p + b^p$ (b) $(a+b)^{p^f} = a^{p^f} + b^{p^f}$

PROBLEM 1 3 Prove that the only automorphism of a prime field is the identity automorphism

2 CONJUGATE ELEMENTS AND AUTOMORPHISMS OF FIELDS

DEFINITION 2 1 If K is a field containing a field F as a subfield then an automorphism α of K is an F *automorphism* of K (also called an automorphism of K over F) $\Leftrightarrow \forall f \in F$ $f^\alpha = f$ If F is a subfield of the fields K and L then an isomorphism α of K onto L is an F *isomorphism* $\Leftrightarrow \forall f \in F$ $f^\alpha = f$

PROBLEM 2.1. Prove that if Π is the prime subfield of a field K, then every automorphism of K is a Π-automorphism.

PROBLEM 2.2. Prove that the isomorphisms between stem fields and splitting fields of Theorem 15.3 of Chapter 5 are F-isomorphisms.

THEOREM 2.1. Let F be a subfield of the fields K and L, and α an F-isomorphism of K onto L. Then, if $\theta \in K$ is a zero of $f(x) \in F[x]$, θ^α is a zero of $f(x)$.

PROOF: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Then $a_0 + a_1\theta + \cdots + a_n\theta^n = 0$ and so $0 = 0^\alpha = (a_0 + a_1\theta + \cdots + a_n\theta^n)^\alpha = a_0^\alpha + a_1^\alpha\theta^\alpha + \cdots + a_n^\alpha(\theta^\alpha)^n = a_0 + a_1\theta^\alpha + \cdots + a_n(\theta^\alpha)^n = f(\theta^\alpha) = 0$. ■

THEOREM 2.2. If the fields K and L are of finite degree over the field F, if α is an F-isomorphism of K onto L, if $\theta \in K$, and if $\theta' = \theta^\alpha$, then $\exists f(x) \in F[x]$, where $f(x)$ irreducible in $F[x] \ni f(\theta) = f(\theta') = 0$.

PROBLEM 2.3. Prove Theorem 2.2. (Hint: use Theorem 12.3 of Chapter 5 and Theorem 2.1 immediately above.)

THEOREM 2.3. If $f(x) \in F[x]$ is irreducible, F is a field, θ_1 and θ_2 are zeros of $f(x)$, and if K is a field containing F, θ_1, and θ_2, then $\exists$ an F-isomorphism, α, of $F(\theta_1)$ onto $F(\theta_2) \ni \theta_2 = \theta_1^\alpha$.

PROOF: This is Theorem 15.2 of Chapter 5 for the case $F = \bar{F}$, $f(x) = \bar{f}(x)$ and α, the identity automorphism of F. ■

THEOREM 2.4. Let K be the splitting field of $f(x)$, irreducible, $\in F[x]$, over F, a field, and let θ_1 and θ_2 be two zeros of $f(x)$. Then $\exists$ an F-automorphism of K which maps θ_1 onto θ_2.

PROBLEM 2.4. Prove Theorem 2.4 by repeated application of Theorem 15.2 of Chapter 5 (cf. proof of Theorem 15.3 of Chapter 5).

DEFINITION 2.2. Let $a, b \in K$, a field containing the field F as a subfield. Then a, b are *conjugates over* $F \Leftrightarrow \exists f(x)$, irreducible, $\in F[x] \ni f(a) = f(b) = 0$.

THEOREM 2.5. Let F, $\bar{F}$ be two isomorphic fields with isomorphism α. Let $f(x) \in F[x]$ and $\bar{f}(x) = [f(x)]^\beta$, where β is the extension of α of Theorem 15.2 of Chapter 5. Finally, let K and $\bar{K}$ be splitting fields of $f(x)$, $\bar{f}(x)$ over F and $\bar{F}$, respectively. Then α can be extended to an isomorphism of K onto $\bar{K}$ in which each zero of $f(x)$ is mapped onto a zero of $\bar{f}(x)$.

PROBLEM 2.5 Prove Theorem 2.5 by repeated application of Theorem 15.1 of Chapter 5.

THEOREM 2.6 Let $f(x)$ be irreducible in $F[x]$, where F is a field, and let K be a splitting field of $f(x)$ over F. Then if $a, b \in K$, $\exists$ an F-automorphism α of $K \ni a = b^{\alpha} \Leftrightarrow a, b$ are conjugates over F.

PROBLEM 2.6 Use Theorem 2.6 to find all the automorphisms of the splitting field of $x^3 - 2 \in Q[x]$. Show that they form a group. Identify the group.

PROBLEM 2.7 Prove Theorem 2.6.

PROBLEM 2.8 Do the same as in Problem 2.6 for $x^4 - 2 \in Q[x]$.

PROBLEM 2.9 Do the same as in Problem 6 for the splitting field of Problem 12.4 of Chapter 5.

3 NORMAL EXTENSIONS OF FIELDS AND NORMAL POLYNOMIALS

DEFINITION 3.1 A *field* K algebraic over a field F is *normal over* $F \Leftrightarrow$ whenever $f(x)$, irreducible in $F[x]$, has a zero in K, then K contains the splitting field of $f(x)$ over F. A *polynomial* $f(x) \in F[x]$, where F is a field and $f(x)$ is irreducible over F, is *normal over* $F \Leftrightarrow \forall\, \theta$, a zero of $f(x)$, $F(\theta)$ is the splitting field of $f(x)$ over F.

PROBLEM 3.1 Show that $x^2 + 3x + 5$ is normal over Q.

PROBLEM 3.2 Show that $ax^2 + bx + c$, irreducible $\in F[x]$, is normal over F.

PROBLEM 3.3 Prove that a field K of degree 2 over a field F is normal over F.

PROBLEM 3.4 Show by an example that, in general, a polynomial $f(x)$ normal over a field F must be irreducible over F.

PROBLEM 3.5 Show that $x^3 - 2$ is not normal over Q and that none of its stem fields is normal over Q.

PROBLEM 3.6 Show that the cyclotomic polynomial $f(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$, where p is a rational prime, is normal over Q. [Hint: each zero of $f(x)$ is a pth root of unity.]

PROBLEM 3.7. Show that the polynomial $x^p - t$ is normal over $F = Z_p(t)$.

THEOREM 3.1. If a field K is normal over a subfield F, then K is normal over every subfield L between K and F (i.e., $K \supset L \supset F$).

PROOF: Let $\phi(x)$ be irreducible in $L[x]$, and suppose that $\phi(\theta) = 0$, where $\theta \in K$. Then, since K is algebraic over F, $\exists f(x)$ irreducible, $\in F[x] \ni f(\theta) = 0$. Then, since K is normal over F, K contains all the zeros of $f(x)$. Since $L \supset F, f(x) \in L[x]$ and $f(x)$ has a zero in common with $\phi(x)$. Therefore, in $K[x]$, $\phi(x)$ and $f(x)$ have a factor $x - \theta$ in common. Hence, in $K[x]$, the g.c.d. of $\phi(x)$ and $f(x)$ has degree $\geqslant 1$. But, the g.c.d. of $f(x)$ and $\phi(x)$ is in $W[x]$, where W is any field containing the coefficients of the two polynomials. Hence, the g.c.d. of $f(x)$ and $\phi(x)$ is in $L[x]$ and is of degree $\geqslant 1$. But $\phi(x)$ is irreducible in $L[x]$. Therefore, $\phi(x) | f(x)$. Thus every zero of $\phi(x)$ is a zero of $f(x)$ and since K contains all the zeros of $f(x)$, it contains all the zeros of $\phi(x)$. Hence, K is normal over L. ■

THEOREM 3.2. Let $f(x) \in F[x]$, where F is a field, and let K be the splitting field of $f(x)$ over F. Then K is a normal extension of F.

PROOF: Let $\phi(x)$ be irreducible in $F[x]$ and let θ_1 be a zero of $\phi(x) \ni \theta_1 \in K$. We must show that all the zeros of $\phi(x) \in K$. Let K' be a splitting field of $\phi(x)$ over K and let θ_2 be any zero of $\phi(x)$. Then, of course, $\theta_2 \in K'$. Since $\phi(x)$ is irreducible in $F[x]$, by Theorem 2.3, $\exists$ an F-isomorphism α of $F(\theta_1)$ onto $F(\theta_2)$ which maps θ_1 onto θ_2. Now K and $K(\theta_2)$ are splitting fields of $f(x)$ over $F(\theta_1)$ and $F(\theta_2)$, respectively. Hence, by Theorem 2.5, the isomorphism α can be extended to an F-isomorphism β of K onto $K(\theta_2)$. Now β is an isomorphism of K into K', a field containing K. Since β is an F-isomorphism and since all the zeros of $f(x)$ are in K, β maps the set of zeros of $f(x)$ onto itself. Therefore, since K is generated by the zeros of $f(x)$, β must be an F-isomorphism of K. Since $\theta_1 \in K$, then $\theta_1{}^\beta = \theta_2 \in K$. Hence, we have proved that each zero of $\phi(x)$ is in K, as long as one zero is in K. Therefore, K is a normal extension of F. ■

THEOREM 3.3. If K is a finite normal extension of a field F, then K is the splitting field of some $f(x) \in F[x]$.

PROBLEM 3.8. Prove Theorem 3.3. (Hint: consider a basis of K over F.)

PROBLEM 3.9. Prove that if $f(x)$ is normal over F, and if θ is a zero of $f(x)$, then $F(\theta)$ is normal over F.

PROBLEM 3.10 Prove that the following is false: if a field K is normal over a field F and if L is a subfield of K, then K is normal over L.

4. SEPARABILITY

DEFINITION 4.1 A *polynomial* $\phi(x) \in F[x]$, where F is a field, is *separable over* $F \Leftrightarrow \phi(x)$ has no multiple zeros in any extension field of F.

An *element* $a \in K$, a field containing F as a subfield, is *separable over* $F \Leftrightarrow a$ is a zero of a polynomial $f(x) \in F[x]$, where $f(x)$ is separable over F.

A *field* K containing F as a subfield is *separable over* $F \Leftrightarrow$ every element of K is separable over F.

Otherwise, the polynomial, element, or field is called *inseparable over* F.

THEOREM 4.1 Let $f(x)$ be an irreducible polynomial of $F[x]$, where F is a field.

(1) If the characteristic of F is zero, then $f(x)$ is separable over F.

(2) If the characteristic of F is $p > 0$, then $f(x)$ is inseparable over $F \Leftrightarrow f(x) = \Sigma_{i=0}^{k} c_i(x^p)^i$, where $c_i \in F$.

PROOF First, we show that if $f(x)$ is inseparable, its derivative $f'(x)$ is zero. By Theorem 2.7 of Chapter 5, if $f(x)$ has a zero of multiplicity greater than 1, then $x - a | f'(x) \Rightarrow f'(a) = 0 \Rightarrow f(x) | f'(x)$, since $f(x)$ is irreducible in $F[x]$, $f'(x) \in F[x]$, and $x - a$ is a common divisor of both $f(x)$ and $f'(x)$. But this is impossible unless $f'(x) = 0$, since $\deg f'(x) < \deg f(x)$ or $f'(x) = 0$. Therefore $f'(x) = 0$.

Now let $f(x) = \Sigma_{i=0}^{n} a_i x^i$ with $a_n \neq 0$. Then $f'(x) = \Sigma_{i=0}^{n} i a_i x^{i-1}$. If $f'(x) = 0$, then we must have $i a_i = 0$ for $i = 0, 1, \ldots, n$. Since $a_n \neq 0$ while $n a_n = 0$, the characteristic of F must be a prime dividing n, so the first statement of the theorem is proved. Now from $i a_i = 0$ for $i = 0, 1, \ldots, n - 1$, we see that $a_i = 0$ if $i \not\equiv 0 \bmod p$. Therefore the only nonzero coefficients of $f(x)$ are a_i, where $i \equiv 0 \bmod p$, and, of course, some of these may be zero. Therefore $f(x) = \Sigma_{j=0}^{k} a_{jp} x^{jp} = \Sigma_{i=0}^{k} c_i(x^p)^i$, where $k = n/p$ and $c_i = a_{ip}$.

Now let $f(x) = \Sigma_{i=0}^{k} c_i(x^p)^i$ and $g(x) = \Sigma_{i=0}^{k} c_i x^i$. Then $f(x) = g(x^p)$. Now $g(x)$ may be a polynomial in x^p; if it is, then $f(x)$ is a polynomial in x^{p^2}, and so on. Suppose finally that $f(x)$ is a polynomial in x^{p^e} but not in $x^{p^{e+1}}$. Then $f(x) = h(x^{p^e})$ and $h(y)$ is irreducible in $F[y]$, since $f(x)$ is irreducible in $F[x]$. Further, $h(y)$ has no multiple zeros, since if $h'(y) = 0$, then by the above $h(y)$ would be a poly nomial in y^p and so $f(x)$ a polynomial in $x^{p^{e+1}}$. In a splitting field of $h(y)$, $h(y) = (y - a_1)(y - a_2) \cdots (y - a_r)$, where the $a_1, a_2, \ldots, a_r$ are distinct. Let, in some further extension field, b_i be a zero of $x^p - a_i$ for $i = 1, 2, \ldots, r$. Then $b_i^{p^e} = a_i$, $x^{p^e} - a_i = x^{p^e} - b_i^{p^e} = (x - b_i)^{p^e}$ and so, since the b_i are distinct because the a_i are, $f(x)$ is an inseparable polynomial and each of its zeros has the same multiplicity. ■

COROLLARY 4.1. The zeros of an irreducible inseparable polynomial $f(x) \in F[x]$ are all of the same multiplicity.

DEFINITION 4.2. If $f(x)$ of degree n is an irreducible, inseparable polynomial $\in F[x]$, where F is a field, and if $f(x) = h(x^{p^e})$, where $h(y) \in F[y]$, while $\nexists\, k(y) \in F[y] \ni f(x) = k(x^{p^{e+1}})$, then $n_0 = n/p$ is called the *reduced degree* of $f(x)$.

PROBLEM 4.1. Show that the polynomial of Problem 3.7 is inseparable. Factor it and find its reduced degree.

PROBLEM 4.2. Find an inseparable polynomial of reduced degree 5.

THEOREM 4.2. K is a separable algebraic extension of a field F, L is a field between K and $F \Rightarrow K$ is separable over L.

THEOREM 4.3. Let K be a finite normal extension of a field F, and θ_1 and θ_2 be two elements of K which are conjugate over F. Then $\exists$ an F-automorphism of K which maps θ_1 onto θ_2.

PROOF: By Theorem 3.3, K is a splitting field over F of some polynomial $f(x) \in F[x]$. Then θ_1 and θ_2 are zeros of some irreducible polynomial, $g(x)$, $\in F[x]$. Then by Theorem 15.3 (a) of Chapter 5, $\exists$ an F-isomorphism α of $F(\theta_1)$ onto $F(\theta_2) \ni \theta_1{}^\alpha = \theta_2$. Since K is the splitting field of $f(x)$ over $F(\theta_1)$ and K is also the splitting field of $f(x)$ over $F(\theta_2)$, the isomorphism α can, by Theorem 2.5, be extended to an F-automorphism of K. ■

THEOREM 4.4. Let K be a finite, normal, separable extension of a field F. If an element $\theta \in K$ is mapped onto itself by all F-automorphisms of K, then $\theta \in F$.

PROOF: Under the given conditions, by Theorem 4.3, θ must coincide with all its conjugates. Thus its minimum polynomial $f(x) \in F[x]$ would factor in K as $f(x) = (x - \theta)^m$. But this would mean, unless $m = 1$, that $f(x)$ irreducible in $F[x]$ would have a multiple zero and, by hypothesis, θ was separable. Therefore, $m = 1$ and so $\theta \in F$. ■

Problem 4 3 Prove Theorem 4 2

Problem 4 4 Show by an example the necessity of separability in Theorem 4 4 (Hint cf Problems 3 7 and 4 1)

Problem 4 5 Determine whether the following is true L is normal over K K is normal over $F \Rightarrow L$ is normal over F

5 SUBFIELDS AND AUTOMORPHISMS

In this section we consider the relations between subfields of a field K and subgroups of the groups of automorphisms of K First of course we must prove that the automorphisms do form a group

Theorem 5 1 The set Ω of automorphisms of a field F and the law of composition of Definition 2 1 of Chapter 2 form a group

Proof Since Ω is a subset of the group of Theorem 7 1 of Chapter 2 and the law of composition is the same we know that the associative law holds Let α $\beta \in \Omega$ Then $\forall$ a $b \in F$ $(a+b)^{\alpha\beta} = [(a+b)^{\alpha}]^{\beta} = [a^{\alpha}+b^{\alpha}]^{\beta} = (a^{\alpha})^{\beta} + (b^{\alpha})^{\beta} = a^{\alpha\beta} + b^{\alpha\beta}$ by the properties of automorphisms and the definition of the product of two mappings Similarly $(ab)^{\alpha\beta} = a^{\alpha\beta}b^{\alpha\beta}$ Therefore Ω is closed The identity mapping is obviously an automorphism of F and clearly is the neutral element of Ω Now for $\beta \in \Omega$ a $b \in F$ let $x = a^{\beta^{-1}}$ $y = b^{\beta^{-1}}$ Then $[a+b]^{\beta^{-1}} = [x^{\beta}+y^{\beta}]^{\beta^{-1}} = [(x+y)^{\beta}]^{\beta^{-1}} = x+y = a^{\beta^{-1}} + b^{\beta^{-1}}$ Similarly $(ab)^{\beta^{-1}} = a^{\beta^{-1}}b^{\beta^{-1}}$ Hence β^{-1} as the mapping inverse to β is in Ω Hence each element of Ω has an inverse Therefore Ω is a group ∎

Theorem 5 2 Let F be a subfield of the field K Then the F automorphisms of K form a subgroup Δ of the group Ω of all automorphisms of K

Proof We shall use Theorem 8 1 of Chapter 3 Let α β be F automorphisms of K Then $\forall f \in F$ $f^{\alpha} = f$ $f^{\beta} = f$ $f^{\beta^{-1}} = f$ Therefore $f^{\alpha\beta^{-1}} = (f^{\alpha})^{\beta^{-1}} = f^{\beta^{-1}} = f$ Therefore $\alpha\beta^{-1} \in \Delta$ Therefore Δ is a subgroup of Ω ∎

Theorem 5 3 Let M be any subset of a field K The set of all automorphisms ξ of $K \ni \forall m \in M$ $m^{\xi} = m$ form a group

Problem 5 1 Prove Theorem 5 3

Problem 5 2 Generalize Theorem 5 3 to F automorphisms of K where F is any subfield of K

Problem 5.3. For $K = Q(\omega, \theta)$ of Problem 13.6 of Chapter 5, (a) find all subfields of K (there are four besides K and its prime subfield), (b) for each subfield (use all six) F of K, find all the F-automorphisms of K.

Problem 5.4. Do the same as in Problem 5.3 for the splitting field of $x^4 - 2$.

Theorem 5.4. Let Λ be any set of automorphisms of a field K. Then the set L of all elements $x \in K \ni \forall \lambda \in \Lambda, x^\lambda = x$, is a subfield of K.

Proof: Let $\alpha \in \Lambda$ and let L_α be the set of all $x \in K \ni x^\alpha = x$. Further, let $a, b \in L_\alpha$. Then $a^\alpha = a, b^\alpha = b$. So $(-b)^\alpha = -b$, since $[b + (-b)]^\alpha = 0 = b^\alpha + (-b)^\alpha = b + (-b)$ and $b^\alpha = b$. Finally, since α is an automorphism of K, $(a - b)^\alpha = [a + (-b)]^\alpha = a^\alpha + (-b)^\alpha = a - b$. Therefore, by Theorem 8.1 of Chapter 3, L_α is a subgroup of the additive group of K.

If $b \neq 0, b^{-1} \in K$, and from $bb^{-1} = 1$, we have $1 = 1^\alpha = (bb^{-1})^\alpha = b^\alpha(b^{-1})^\alpha = b(b^{-1})^\alpha \Rightarrow (b^{-1})^\alpha = b^{-1}$, since the multiplicative inverse of b is unique. Therefore, $(ab^{-1})^\alpha = ab^{-1}$, and so, the nonzero elements of L_α form a subgroup of the multiplicative group of K. Therefore, L_α is a subfield of K. ■

Problem 5.5. For each subgroup Λ of the group of automorphisms of the field of Problem 5.3, find the subfield whose existence is given by Theorem 5.4.

Problem 5.6. Same as Problem 5.5 for the field of Problem 5.4.

Definition 5.1. Let K be a field and Γ its group of automorphisms.

If Λ is a subgroup of Γ, $N(\Lambda)$ is the subfield of K determined in Theorem 5.4 and is called the *subfield belonging to* Λ.

If L is a subfield of K, $\Omega(L)$ is the subgroup of Γ determined in Theorem 5.3 and is called the *subgroup belonging to L.*

The above may also be considered for Γ as the group of F-automorphisms of K, where F is a subfield of K.

Problem 5.7. Apply the terminology of Definition 5.1 to the results of Problems 5.3, 5.4, 5.5, and 5.6.

Problem 5.8. Do Problems 5.3 and 5.5 for the smallest field containing the splitting fields of $x^2 - 2$ and $x^3 - t$ as elements of $Z_3(t)[x]$.

THEOREM 5 5   Let K be a field and Γ its group of automorphisms For any subgroup Λ of Γ $\Omega(N(\Lambda)) \supset \Lambda$ and for any subfield L of K $N(\Omega(L)) \supset L$

THEOREM 5 6   Let K be a field and Γ its group of automorphisms If Λ_1 Λ_2 are subgroups of $\Gamma \ni \Lambda_1 \subset \Lambda_2$ then $N(\Lambda_1) \supset N(\Lambda_2)$ if L_1 L_2 are subfields of $K \ni L_1 \subset L_2$ then $\Omega(L_1) \supset \Omega(L_2)$

PROBLEM 5 9   Prove Theorem 5 5

PROBLEM 5 10   Prove Theorem 5 6

PROBLEM 5 11   Give an example in which the strict inclusion is necessary in the second conclusion of Theorem 5 5 (Hint use Problem 3 7)

6 ROOTS OF UNITY

DEFINITION 6 1   Let Π be a prime field and n a positive rational integer not divisible by the characteristic of Π if the characteristic of Π is zero n may be any positive rational integer Then an *nth root of unity* is any zero of $f(x) = x^n - 1$ in any extension field of Π The splitting field of this $f(x)$ is called the field of the *nth roots of unity* over the prime field Π and is also called the *cyclotomic field of order n*

THEOREM 6 1   In the field of the nth roots of unity there are exactly n distinct nth roots of unity and they form a multiplicative cyclic group

PROOF   By Corollary ? 2 in Chapter 5 the zeros of $f(x) = x^n - 1$ are distinct since $f'(x) = nx \neq 0$ since $p \nmid n$ where p is the characteristic of Π if it is not zero Therefore there are n distinct nth roots of unity

Let α and β be two such ie α 1 $\beta = 1$ then $(\alpha/\beta)^n = 1$ and so the nth roots of unity form a multiplicative group G

Let $n = \Pi^m$ p where the p are distinct primes $i = 1$ 2 m In G there are at most n/p elements $\ni a$ $^p = 1$ since the polynomial $x^{n/p} - 1$ has at most n/p zeros Therefore $\forall i < m$ $\exists c \in G \ni a$ $^p \neq 1$ Let $b = a$ ^{p} Then b has period p for since b $= 1$ its period must be a factor of p But b $= (a^{n/p})^p$ $= a^{n/p} \neq 1$ Thus the product $\zeta = \Pi_=$ b has period $\Pi^m{}_1 p_i^r = n$ Therefore ζ generates G and so G is cyclic ■

DEFINITION 6 2   A generator of the cyclic group of the nth roots of unity is called a ***primitive nth root of unity***

Corollary 6.1. $\exists\ \phi(n)$ primitive nth roots of unity.

Definition 6.3. The polynomial $\Phi_n(x) = (x - \zeta_1)(x - \zeta_2) \cdots (x - \zeta_{\phi(n)})$, having as its zeros the primitive nth roots of unity is called the *cyclotomic polynomial of order* n.

Theorem 6.2. $x^n - 1 = \Pi_{d|n} \Phi_d(x)$.

Proof: Each nth root of unity is a primitive dth root of unity for exactly one divisor d of n. Therefore, it occurs as a zero of exactly one $\Phi_d(x)$ on the right, and it of course occurs in exactly one factor (linear) of $x^n - 1$. ■

Problem 6.1. Find $\Phi_2(x)$, $\Phi_4(x)$, $\Phi_8(x)$, $\Phi_3(x)$, $\Phi_6(x)$.

Problem 6.2. Prove that if ζ is an nth root of unity, $1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = n$ if $\zeta = 1$ and 0 if $\zeta \neq 1$.

Problem 6.3. Prove that if n is odd, the field of the nth roots of unity is the field of the $(2n)$th roots of unity.

Problem 6.4. Prove that $\Phi_n(x)$ is normal over the prime field Π (cf. Problem 3.6).

7. FINITE FIELDS

Definition 7.1. A *finite field* is a field containing only a finite number of distinct elements. Such a field is often called a *Galois Field* and is usually denoted by $GF(p^n)$ where p^n is the number of elements in it (cf. Theorem 7.1 below). The *order* of a finite field is the number of elements in it.

Theorem 7.1. The number of elements in a finite field F is p^n, where p is the characteristic of F and $n \in Z^+$.

Proof: Obviously by Theorem 1.3, the characteristic of F cannot be zero and so by Theorem 1.1 must be a positive rational prime p.

Let Π be the prime subfield of F. Then F is a vector space over Π, and, if the number of elements in F is q, then there are at most q linearly independent elements in F. Let n be the number of elements in a maximum set of linearly independent elements, and let $a_1, a_2, \ldots, a_n$ be such a set. Then $a_1, a_2, \ldots, a_n$ form a basis of F over Π, so every element of F can be expressed uniquely in the form $c_1a_1 + \cdots + c_na_n$, where the $c_i \in \Pi$. These elements are all distinct, by the uniqueness property of a basis. There are exactly p^n of them, since

c_i can be any of the p elements of Π. Therefore F contains exactly p elements. ■

THEOREM 7.2 If F is a finite field of order p^n, then every element of F is a zero of $x^{p^n} - x$.

PROOF The nonzero elements of F form a multiplicative group which is of order $p^n - 1$ and so each element satisfies $x^{p^n - 1} - 1 = 0$. Therefore every element of F including zero is a zero of $x^{p^n} - x$. ■

THEOREM 7.3 If F is a finite field of order p^n, then the multiplicative group of F consists of the $(p^n - 1)$th roots of unity over the prime field of characteristic p.

PROOF $p \nmid p^n - 1$ and by Theorem 7.2 every nonzero element of F satisfies $x^{p^n - 1} - 1 = 0$. ■

COROLLARY 7.1 Two finite fields of order p^n are isomorphic.

COROLLARY 7.2 The multiplicative group of $\mathrm{GF}(p^n)$ is cyclic.

THEOREM 7.4 For each positive rational prime p and each $n \in Z^*$ $\exists$ a finite field $\mathrm{GF}(p^n)$.

COROLLARY 7.3 Let $\Pi = \mathrm{GF}(p)$ and $n \in Z^*$. $\exists f(x) \in \Pi[x] \ni$

(1) $\deg f(x) = n$

(2) $f(x)$ is irreducible in $\Pi[x]$

PROBLEM 7.1 Prove Theorem 7.4 (Hint: let K be the splitting field of $x^{p^n} - x$ over Π. By using problem 1.2 show that the zeros of this polynomial form a field which must be K.)

PROBLEM 7.2 Prove the three corollaries above.

PROBLEM 7.3 Prove: let $\Pi = \mathrm{GF}(p)$ and let $f(x) \in \Pi[x]$. Then $[f(x)]^{p^m} = f(x^{p^m})$ $\forall m \in Z^*$.

DEFINITION 7.2 $\theta \in K \supset F$ is a *primitive element of the field K over the field $F \Leftrightarrow K = F(\theta)$*.

THEOREM 7.5 $\mathrm{GF}(p^n)$ is a simple extension of Π, its prime field (which is $\mathrm{GF}(p)$).

PROOF Since by Corollary 7.2 the multiplicative group of $\mathrm{GF}(p^n)$ is cyclic, $\exists$ a generator θ for it. Then $\mathrm{GF}(p^n) = \Pi(\theta)$. ■

THEOREM 7.6 The mapping α_m defined by $x^{n} = x^{p^m}$ is an automorphism of $\mathrm{GF}(p^n)$ and these n automorphisms are distinct.

PROBLEM 7.4. Prove Theorem 7.6.

8. PRIMITIVE ELEMENTS

THEOREM 8.1. (The Primitive Element Theorem.)
(1) $\rho, \sigma \in K$, a field containing the field F as a subfield,
(2) ρ, σ are algebraic over F,
(3) σ is separable over $F \Rightarrow \exists\, \theta \in K \ni F(\theta) = F(\rho, \sigma)$.

PROOF: Let $f(x)$, $g(x)$ be the minimum polynomials of ρ, σ, respectively, over F and let $\rho = \rho_1, \rho_2, \ldots, \rho_r$ and $\sigma = \sigma_1, \sigma_2, \ldots, \sigma_s$ be the distinct zeros of $f(x)$ and $g(x)$, respectively.

Since, if F is a finite field, so is $F(\rho, \sigma)$ and Theorem 7.5 covers this case, we may suppose that F has infinitely many elements.

Since the σ_k are all distinct, the equation $\rho_i + x\sigma_k = \rho_1 + x\sigma_1$, $k \neq 1$, has at most one root in F for each i, k, namely, $(\rho_i - \rho_1)/(\sigma_1 - \sigma_k)$, if this element $\in F$. There are thus at most $r(s-1)$ elements which can be roots of these $r(s-1)$ equations. Let c be any other element of F. Then we have $\rho_i + c\sigma_k \neq \rho_1 + c\sigma_1$ for all i and for all $k \neq 1$. Let $\theta = \rho_1 + c\sigma_1 = \rho + c\sigma$. Then $\theta \in F(\rho, \sigma)$ and so $F(\theta) \subset F(\rho, \sigma)$.

We shall now prove that $\rho \in F(\theta)$, $\sigma \in F(\theta)$, and so $F(\rho, \sigma) \subset F(\theta)$. Then we can conclude that $F(\theta) = F(\rho, \sigma)$.

Now σ is a zero of $g(x)$ and $f(\theta - cx)$, since $f(\theta - c\sigma) = f(\rho) = 0$, and these two polynomials, $g(x), f(\theta - cx) \in F(\theta)[x]$. Furthermore, the only zero which $g(x)$ and $f(\theta - cx)$ have in common is σ, since for the other zeroes $\sigma_2, \ldots, \sigma_s$ of $g(x)$ we have $\theta - c\sigma_k \neq \rho_i; i = 1, \ldots, r; k = 2, 3, \ldots, s$, and so $f(\theta - c\sigma_k) \neq 0$ for $k = 2, 3, \ldots, s$. Therefore, a g.c.d. of $g(x)$ and $f(\theta - cx)$ is $x - \sigma$ and this must belong to $F(\theta)[x]$, since $f(\theta - cx)$ and $g(x) \in F(\theta)[x]$. Therefore, $\sigma \in F(\theta)$. Since $\rho = \theta - c\sigma$, $c \in F$, then $\rho \in F(\theta)$. ■

COROLLARY 8.1. If $\tau_1, \tau_2, \ldots, \tau_m$ are algebraic over F, and $\tau_2, \ldots, \tau_m$ are separable over F, then $\exists\, \theta \in F(\tau_1, \ldots, \tau_m) \ni F(\theta) = F(\tau_1, \ldots, \tau_m)$.

COROLLARY 8.2. $\theta \in K \supset F$ is a primitive separable element of K over F, where $[K:F] = n \Leftrightarrow$ the degree of the minimum polynomial of θ is $n \Leftrightarrow \theta$ has n distinct conjugates over F.

PROBLEM 8.1. Prove Corollaries 8.1 and 8.2.

PROBLEM 8.2. State carefully where, in the proof of Theorem 8.1, the separability of σ was used.

PROBLEM 8 3 Use the method of the proof of Theorem 8 1 to find primitive elements for each of the following fields (in each case over the prime field) (a) $Q(\sqrt{2}\ \sqrt{3})$ (b) $Q(\sqrt{3}\ i)$ (c) $Q(\sqrt[3]{2}\ i)$ (d) $Q(\sqrt[4]{2}\ i)$ Prove in each case that the element found is a primitive element

DEFINITION 8 1 If θ is a primitive element of the field K over the field F then a polynomial $p(x)$ irreducible in $F[x]$ and $\ni p(\theta) = 0$ is called a *Galois resolvent* of K over F If K is the splitting field of $f(x) \in F[x]$ over F $p(x)$ is also called the Galois resolvent of $f(x)$

PROBLEM 8 4 Find Galois resolvents for each of the fields of Problem 8 3

THEOREM 8 2 Let $K = F(\theta)$ be normal over F and $f(x)$ of degree n be the minimum polynomial of θ over F Then $\exists$ exactly n F automorphisms of K if θ is separable over F and n_0 where n_0 is the reduced degree of $f(x)$ F automorphisms of K if θ is inseparable over F

PROOF Since K is normal over F K contains all the conjugates over F of θ and these are the zeros of $f(x)$ Since $K = F(\theta)$ any F automorphism of K is uniquely determined by specifying the image of θ By Theorem 2 6 θ must be mapped onto one of its n (or n_0) conjugates Therefore $\exists$ at most n (or n_0) F automorphisms But the n (or n_0) conjugates are distinct and so again by Theorem 2 6 for each conjugate $\exists$ an F automorphism of K Therefore $\exists$ at least n (or n_0) F automorphisms Therefore exactly n (or n_0) ∎

COROLLARY 8 3 If K is the splitting field of $f(x) \in F[x]$ over F where $f(x)$ is separable and irreducible in $F[x]$ $\exists$ exactly n F automorphisms of K where $n = [K\ F]$

COROLLARY 8 4 If K is a finite normal separable extension of F of degree n over F $\exists$ exactly n F automorphisms of K

PROBLEM 8 5 Prove the Corollaries 8 3 and 8 4

9 THE GALOIS THEORY OF FIELDS

DEFINITION 9 1 A field K is a *Galois extension* of a subfield $F \Leftrightarrow K$ is finite normal separable over F

We shall often say briefly that K is Galois over F if and only if K is a Galois extension of F

Definition 9.2. If K is Galois over F, the group of F-automorphisms of K is called the *Galois group of K over F*. If $f(x)$ is a separable polynomial of $F[x]$, K its splitting field, then the Galois group of K over F is called the *Galois group of the polynomial* $f(x)$ [or of the equation $f(x) = 0$].

Theorem 9.1. If K is Galois over F, and L a subfield of K containing F, then $N(\Omega(L)) = L$.

Proof: (cf. Theorem 5.5.) By Theorem 3.1, K is normal over L, and by Theorem 4.2, K is separable over L, and so K is Galois over L. We can, therefore, apply Theorem 4.4 with the F of that theorem replaced by our present L. ■

Theorem 9.2. If K is Galois over F, Γ, it is Galois group over F, and Λ any subgroup of Γ, then $\Omega(N(\Lambda)) = \Lambda$.

Proof: By Theorem 5.5, $\Omega(N(\Lambda)) \supset \Lambda$, so if $\Omega(N(\Lambda)) \neq \Lambda$, then $\exists$ at least one $\omega \in F \ni \forall x \in N(\Lambda)$, $x^\omega = x$, while $\omega \notin \Lambda$. This means, i.e., if $\omega \notin \Lambda$, there must exist some element $a \in K \ni a^\omega = a$ while for at least one $\lambda_0 \in \Lambda$, $a^{\lambda_0} \neq a$. Then $a \notin N(\Lambda)$, while $a \in N(\Omega(N(\Lambda)))$. But, by Theorem 9.1, $N(\Omega(N(\Lambda))) = N.(\Lambda)$. Therefore, no such ω exists and so $\Omega(N(\Lambda)) = \Lambda$. ■

Theorem 9.3. If K is Galois over F, Γ the Galois group of K over F, if the subfield $L \supset F$ belongs to the subgroup, Λ, then the order of Λ is equal to the degree of K over L, and the index of Λ in Γ is equal to the degree of L over F.

Problem 9.1. Prove Theorem 9.3.

Problem 9.2. Verify Theorems 9.1, 9.2, and 9.3 for the splitting fields of $x^3 - 2$ and $x^4 - 2$.

Theorem 9.4. Let K be Galois over F. Then two subfields L_1, L_2 of K, each containing F, are conjugates over $F \Leftrightarrow \Omega(L_1), \Omega(L_2)$ are conjugate subgroups of Γ, the Galois group of K over F.

Proof: Let $\Lambda_1 = \Omega(L_1)$, $\Lambda_2 = \Omega(L_2)$.

Consider the implication $\Rightarrow$. By hypothesis, $\exists\ \alpha \in \Gamma \ni L_1{}^\alpha = L_2$. Let $\lambda \in \Lambda_1$. Then $\forall x \in L_1, x^\lambda = x$. Let $y_1 \in L_2$, and $y_1{}^{\alpha^{-1}} = x_1 \in L_1$. Then we have $y_1{}^{\alpha^{-1}\lambda\alpha} = x_1{}^{\lambda\alpha} = (x_1{}^\lambda)^\alpha = x_1{}^\alpha = y_1 \Rightarrow \alpha^{-1}\lambda\alpha \in \Lambda_2$, $\forall \lambda \in \Lambda_1$. Similarly, $\forall \lambda' \in \Lambda_2$, $\alpha\lambda'\alpha^{-1} \in \Lambda_1$. Therefore, $\alpha^{-1}\Lambda_1\alpha = \Lambda_2$.

Now consider the implication $\Leftarrow$. By hypothesis, $\exists\ \alpha \in \Gamma \ni \alpha^{-1} \Lambda_1 = \Lambda_2$. Now α maps L_1 onto some conjugate subfield $\bar{L}$. Let $\bar{y} \in \bar{L}$

and $x_1 = y^{\alpha^{-1}}$ Then $\forall \lambda \in \Lambda_1$, $y^{\alpha^{-1}\lambda\alpha} = x_1^{\lambda\alpha} = x_1^{\alpha} = y$ Therefore, $L_2 = N(\Lambda_2) \supset \bar{L}$ Therefore $L_2^{\alpha^{-1}} \supset \bar{L}^{\alpha^{-1}}$ But, since Λ_1 and Λ_2 are conjugate, they have the same order Therefore, by Theorem 9 3, $L_2^{\alpha^{-1}} = L_1$, $L_1^{\alpha} = L_2$ Therefore, L_1 and L_2 are eonjugate ∎

THEOREM 9 5 Let K be Galois over F A subfield L of K is normal over $F \Leftrightarrow L$ coincides with its conjugate subfields under all F automorphisms of K

PROBLEM 9 3 Prove Theorem 9 5 (Hint use Theorem 2 6 and the pertinent definitions)

THEOREM 9 6 Let K be Galois over F A subfield L of K is normal over $F \Leftrightarrow \Omega(L)$ is a normal subgroup of Γ the Galois group of K over F A subgroup Λ of Γ is normal $\Leftrightarrow N(\Lambda)$ is normal over F

PROBLEM 9 4 Prove Theorem 9 6 using Theorems 9 4 and 9 5

PROBLEM 9 5 Prove Theorem 9 6 by using the method of the proof of Theorem 9 4

PROBLEM 9 6 Examine the splitting fields of $x^3 - 2$ and $x^4 - 2$ in light of Theorems 9 3 4 5 6

THEOREM 9 7 Let K be Galois over F Let L be a subfield of K normal over F and let $\Lambda = \Omega(L)$ Then the Galois group of L over F is isomorphic to Γ/Λ where Γ is the Galois group of K over F Λ is the Galois group of K over L

PROBLEM 9 7 Prove Theorem 9 7

PROBLEM 9 8 Apply Theorem 9 7 to the splitting fields of $x^3 - 2$ and $x^4 - 2$

10 THE CYCLOTOMIC FIELD

The cyclotomic field of order n was defined earlier for a prime field Π We now generalize that

DEFINITION 10 1 The field C_n is called the *cyclotomic extension field of order n* over the field $F \Leftrightarrow C_n$ is the smallest field containing F and all the nth roots of unity

We shall throughout the rest of this chapter assume that the characteristic of F does not divide n

THEOREM 10 1 C_n exists for each field F and is a finite normal and separable extension of F Further the Galois group of C_n over F

is isomorphic to the multiplicative group of the reduced residue classes modulo n.

PROOF: We leave the proof of the first statement of the theorem to the reader as an exercise.

The primitive elements of C_n over F are the powers, ζ^k, where ζ is a primitive nth root of unity and $k \in Z^* \ni (k, n) = 1$, and so $C_n = F(\zeta^k)$, $(k, n) = 1$. Thus we can determine each F-automorphism of $K = F(\zeta)$ by determining the image of ζ, which must be a primitive nth root of unity so we have a 1–1 mapping of the F-automorphisms onto the reduced residue classes modulo n. Further, if we let α_k be the F-automorphism $\zeta \Leftrightarrow \zeta^k$, for $(k, n) = 1$, we have $\alpha_k\alpha_h$ determined by $\zeta \Leftrightarrow (\zeta^k)^h = \zeta^{kh}$, where $(h, n) = 1$, and if we let $kh \equiv w \bmod n$, then $(w, n) = 1$, and $\zeta^{kh} = \zeta^w$, and so we have the desired automorphism. ■

COROLLARY 10.1. The Galois group of C_n over F is the direct product of cyclic groups.

DEFINITION 10.2. The field K, Galois over the field F, is called *cyclic over* $F \Leftrightarrow$ the Galois group of K over F is cyclic. In accordance with Definition 9.1, we call a polynomial or an equation cyclic $\Leftrightarrow$ its Galois group is cyclic.

COROLLARY 10.2. If p is a positive rational prime and F is a field of characteristic different from p, then C_p over F is cyclic over F and $[C_p : F] | p - 1$.

PROBLEM 10.1. Prove the first statement of Theorem 10.1.

PROBLEM 10.2. Prove Corollaries 10.1 and 10.2.

LEMMA. $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$, F a field, $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ in $K[x]$, where K is the splitting field of $f(x)$ over $F \Rightarrow \alpha_1\alpha_2 \cdots \alpha_n = (-1)^n a_0$.

PROBLEM 10.3. Prove the above lemma.

THEOREM 10.2. Let p be a positive rational prime, and let $f(x) = x^p - a$, where $a \in F$, a field, $a \neq 0$. Then the splitting field K of $f(x)$ over F contains the cyclotomic field C_p over F, and exactly one of the following statements holds:

(1) $x^p - a$ has a zero in F, i.e., $\exists\, b \in F \ni b^p = a$. Then $x^p - a$ is reducible in $F[x]$ and $C_p = K$;

(2) $x^p - a$ does not have a zero in F. Then $x^p - a$ is irreducible in $F[x]$ and also in $C_p[x]$. Further, it is normal over C_p, and $K = C_p(\alpha)$, where α is any zero of $x^p - a$.

PROOF Let α_1 α_2 α_p be the zeros of $x - a$ and α any one of them Since $a \neq 0$ $\alpha \neq 0$ and we have since $\alpha = a$

$$\left(\frac{x}{\alpha}\right) - 1 - \left(\frac{x^p - a}{\alpha^p}\right) = \left(\frac{x - \alpha_1}{\alpha}\right) \quad \left(\frac{x - \alpha_j}{\alpha}\right)$$

$$- \left(\frac{x}{\alpha} - \frac{\alpha}{\alpha}\right) \quad \left(\frac{x}{\alpha} - \frac{\alpha_p}{\alpha}\right)$$

Letting $y = x/\alpha$ we have

$$y - 1 - \left(y - \frac{\alpha_1}{\alpha}\right)\left(y - \frac{\alpha_2}{\alpha}\right) \quad \left(y \quad \frac{\alpha}{\alpha}\right)$$

and so $\alpha\ /\alpha$ are the pth roots of unity Therefore $K \supset C_p$

Further if ζ is a primitive pth root of unity we have $\alpha = \zeta\alpha$ $i - 1\ 2$ p remembering the α if necessary

Case (1) Here some one at least of the $\alpha \in F$ and we choose that one as α and then by the above all the $\alpha \in C_p$ and $K \subset C_p$ Therefore $K - C$

Case (2) Here none of the $\alpha \in F$ Suppose $x^p - a - g(x)h(x)$ and we may suppose that $g(x)$ is irreducible in $F[x]$ say $g(x) - x^k + a_k\ x^k + \quad + a\ x + a_0$ where $k < p$ Then by the above lemma $\pm a_0$ would be a product of k of the α and so by the above representation of the α $+ a - \zeta^h\zeta^k$ Since $k < p$ $(k\ p) - 1$ and so $\exists s\ t \in Z$ $\ni sk - 1 + tp$ and since $\alpha - a$ we would have $(\pm a_0) - \zeta^{hs}\alpha\epsilon$ and so since $a \neq 0$ the zero $\alpha_{hs} - \zeta^{hs}\alpha - (\pm\epsilon\ )/a^t$ is in F contrary to our hypothesis that none of the $\alpha \in F$ Therefore $x^p\ \ a$ in this case is irreducible in $F[x]$ and so $[F(\alpha)\ F] - p$ Now if in the above discussion we had assumed that the factorization of $x^p - a$ were in $C_p[x]$ we would have concluded that $\alpha \in C_p$ and so $F(\alpha) \subset C_p$ Then we would have the degree of C_p over F a multiple of p by Theorem 13 3 of Chapter 5 while by Corollary 10 1 $[C_p\ F] | p - 1$ a contradiction Hence in this case $x^p - a$ is also irreducible in $C_p[x]$ Hence $x^p - a$ is clearly normal over C_p so $K = C_p(\alpha)$ ∎

11 PURE EXTENSION FIELDS

DEFINITION 11 1 A *polynomial* (equation) $\in F[x]$ is called *pure* $\Leftrightarrow$ it is of the form $x^n - a$ $(x^n - a - 0)$ $a \in F$ $n \in Z^*$

An *extension field* L of a field K is called *pure* $\Leftrightarrow$ $L - F(\theta)$ where θ is a zero of a pure irreducible F polynomial

THEOREM 11 1 Let p be a positive rational prime and F a field with characteristic $\neq p$ which contains the pth roots of unity over F, then if K is a pure extension of degree p over F, K is normal, separable, and cyclic over F.

PROBLEM 11.1. Prove Theorem 11.1.

THEOREM 11.2. Let p be a positive rational prime, and F a field with characteristic $\neq p$ which contains the pth roots of unity over F, then, if K is a normal extension of degree p over F, K is pure, separable, and cyclic over F.

PROOF: Since $[K:F]=p$, a prime, and K is normal over F, the Galois group is of order p and so is cyclic; let σ be one of its generators. Since $p \neq$ characteristic of F, K is separable over F, and so $\exists$ a primitive element θ of K over F. First, let us suppose that $\exists$ a primitive pth root of unity, ζ, $\ni$ $\alpha = \theta + \zeta\theta^{\sigma} + \zeta^2\theta^{\sigma^2} + \cdots + \zeta^{p-1}\theta^{\sigma^{p-1}}$ $\neq 0$. Then $\alpha^{\sigma} = \theta^{\sigma} + \zeta\theta^{\sigma^2} + \cdots + \zeta^{p-1}\theta = \zeta^{-1}\alpha$, and generally, α^{σ^k} $=\zeta^{-k}\alpha$. Thus the p conjugates of α are all distinct (still assuming $\alpha \neq 0$), and so the minimum polynomial of α is $f(x) = (x-\alpha)(x-\zeta\alpha)$ $\cdots (x-\zeta^{p-1}\alpha)$. Thus as in the proof of Theorem 11.1, $f(x) = x^p - \alpha^p$ and since $f(x) \in F[x]$, $\alpha^p \in F$ and so $F(\alpha) = K$ is a pure extension of F.

Now we must show that ζ can be chosen so that $\alpha \neq 0$. Let us suppose that it is impossible. Then for each choice of a primitive pth root of unity, $\alpha = 0$. The pth roots of unity are all given by ζ^{ι}, $\iota = 1, 2, \ldots, p-1$, where ζ is any one of them. So we have the $p-1$ equations $\theta - \zeta\theta^{\sigma} + \zeta^2\theta^{\sigma^2} + \cdots + \zeta^{p-1}\theta^{\sigma^{p-1}} = 0$, $\theta + \zeta^2\theta^{\sigma} + \zeta^4\theta^{\sigma^2} + \cdots + \zeta^{2(p-1)}\theta^{\sigma^{p-1}} = 0$, $\ldots$, $\theta + \zeta^{p-1}\theta^{\sigma} + \cdots + \zeta^{(p-1)^2}\theta^{\sigma^{p-1}} = 0$, i.e., $\Sigma_{k=0}^{p-1}\zeta^{ik}\theta^{\sigma^{\ k}} = 0$. On multiplying the ith equation by ζ^{-it}, summing over i, and interchanging the order of summation, we have

$$\sum_{k=0}^{p-1}\left(\sum_{\iota=0}^{p-1}\zeta^{\iota(k-t)}\right)\theta^{\sigma^k} = 0.$$

Now $\Sigma_{\iota=1}^{p-1}\zeta^{\iota(k-t)} =$ *either* -1, if $k \neq t$ mod p, since then ζ^{k-t} is a zero of $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ *or* $p-1$, if $k \equiv t$ mod p, since then each term is equal to 1. Thus, the last double summation gives us $\Sigma_{k=0}^{p-1}(-1)\theta^{\sigma^k} + p\theta^{\sigma^t}$ or $p\theta^{\sigma^t} = \Sigma_{k=0}^{p-1}\theta^{\sigma^k}$, but since the characteristic of F is not p, θ^{σ^t} is the same for all $t = 1, 2, \ldots, p-1$. This is impossible, since θ was chosen as a primitive element of K, and σ^t runs through with t all F-automorphisms of K. Therefore, it is possible to choose ζ so that $\alpha \neq 0$. ■

The above theorem implies that a field K satisfying the given conditions can be obtained by adjoining one pth root of a, where a is some element of F. Now we consider a theorem implying something similar about roots of unity.

THEOREM 11.3. Let p be a positive rational prime and F a field whose characteristic is 0 or a prime greater than p. Then for the cyclotomic field C_p over F $\exists$ a finite sequence of fields $L_0, L_1, \ldots, L_r$ $\ni F = L_0 \subset L_1 \subset \cdots \subset L_r \supset C_p \ni L_i$ is pure, normal, and of prime degree over L_{i-1}, $i = 1, 2, \ldots, r$.

PROOF. The theorem is obvious if $p = 2$, since then $C_p = F$.

We now assume that the theorem is true for all primes less than p and for all fields F satisfying the conditions of the theorem. Let d be the degree of C_p over F. Then by Corollary 10.2, $d | p-1$. Let $d = p_1 p_2 \cdots p_k$ be the factorization of d into (not necessarily distinct) primes. Then the characteristic of $F > p_i$, $i = 1, 2, \ldots, k$ and so the induction hypothesis holds. Therefore $\exists$ a finite sequence of fields $F = L_0 \subset L_1 \subset \cdots \subset L_{r_1} \supset C_{p_1}$ in which L_i is pure, normal and of prime degree over L_{i-1}, $i = 1, 2, \ldots, r_1$. Then starting from L_{r_1}, we get another sequence of fields $L_{r_1+1} \subset L_{r_1+2} \subset \cdots \subset L_{r_2} \supset C_{p_2}$ and C_{p_1}. (Naturally C_{p_1} over L_{r_1} contains C_{p_1} over F.) Continuing thus, we get finally a finite sequence of fields $F = L_0 \subset L_1 \subset \cdots \subset L_{r_k}$ where $L_{r_k} \supset C_{p_i}$ for $i = 1, 2, \ldots, k$ over F in which each L_i is pure, normal and of prime degree over L_{i-1} for $i = 1, 2, \ldots, r_k$.

Now let $\bar{C}_p$ be the cyclotomic field over L_{r_k}. By Corollary 10.2 the Galois group Γ of $\bar{C}_p$ over L_{r_k} is cyclic. Therefore, by Problem 14.9 of Chapter 3, the Galois group of $\bar{C}_p$ over L_{r_k} is solvable, so $\exists$ a finite sequence of normal subgroups of Γ: $\Gamma = H_0 \supset H_1 \supset \cdots \supset H_{n+1} = \{\iota\}$ each of which is of prime index in the preceding. Hence, by Theorem 9.4, the subfields $N(H_i) = L_{r_k+i}$ are such that each is of prime degree (= some p_j) over the preceding field, and lastly, by Theorem 11.2, since L_{r_k} and so a fortiori L_{r_k+i} contains all the p_ith roots of unity for $i = 1, 2, \ldots, k$, each field is pure over the preceding. Thus we have $F = L_0 \subset L_1 \subset \cdots \subset L_{r_k} \subset L_{r_k+1} \subset \cdots \subset L_r = \bar{C}_p \supset C_p$ over F and each L_i is pure, normal, and of prime degree over L_{i-1} for $i = 1, 2, \ldots, r$. ∎

12 SOLVABILITY BY RADICALS

By solving an equation by radicals, one naturally means expressing the roots of the equation in terms of the coefficients of the equation using addition, subtraction, multiplication, division, and the extraction of roots of expressions previously formed. For example, an expression which might arise in the process could be something like $\{5 - [3/2 - (4 + 7^{1/2})^{1/8}]^{1/6}\}^{1/7}$. Considering this as occurring from an equation with coefficients $\in Q$, we would first adjoin $7^{1/2}$, getting then a field which contains $4 + 7^{1/2}$. Then to that field we adjoin $(4 + 7^{1/2})^{1/8}$ getting a new field containing $3/2 - (4 + 7^{1/2})^{1/8}$, and so on. Thus at each step we adjoin a root of a pure equation, i.e., of the form, $x^n - a = 0$. Lastly, if in adjoining $a^{1/n}$, n is not a prime, say $n = pq$, where p and q are prime, we can consider it done by two consecutive adjunctions of roots of pure equations of prime degree. Of course, if n is the product of k primes (not necessarily distinct), we do it by k adjunctions, each of prime degree.

Theorem 12.1. (1) If an irreducible equation $f(x) = 0$, where $f(x) \in F[x]$, is solvable by radicals, then the Galois group of the equation is solvable;

(2) if the Galois group of the equation $f(x) = 0$ is solvable, then the equation is solvable by radicals. In both cases, the characteristic of F is to be greater than any prime occurring as an index of a radical or as an index of a group of a composition series, or else the characteristic is to be zero.

Proof: (1) As remarked above we may assume that all roots taken are pth where p is a prime. Let $p_1, p_2, \ldots, p_k$ be all the primes. entering in the expression of the roots of the equation as p_ith roots of elements in successive fields. If we adjoin successively to F the p_1th, p_2th, $\ldots$, p_kth roots of unity we get a succession of fields $F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_k$, each of which by Theorem 10.1 is cyclic over the preceding field. We now adjoin successively all the p_ith roots of all other elements necessary in the expression of the roots by radicals. By Theorem 11.2, each time we get a pure, separable, cyclic, normal extension of prime degree over the preceding field. Thus a chain of fields $F = F_0 \subset F_1 \subset \cdots \subset F_k \subset F_{k+1} \subset \cdots \subset F_h = W$, where each is normal over all those preceding. The final field W contains all the roots of $f(x) = 0$ and is normal over F, and it contains the splitting field K of $f(x)$. Now let Ω be the Galois group of W over F. Then, corresponding to the chain of fields given above, we have a chain of subgroups of Ω, $\Omega = \Gamma_0 \supset \Gamma_1 \supset \cdots \supset \Gamma_h = \{\iota\}$, and each of these subgroups is invariant in the preceding and Γ_i/Γ_{i+1} is cyclic and of prime order. To the field K belongs some subgroup of Ω, say Λ, and by Theorem 9.6, Λ is an invariant subgroup of Ω. We can find another (perhaps the same if $\Lambda = \Gamma_i$ for some i) composition series for Ω which contains Λ and whose quotient groups are isomorphic to those of the original composition series, $\Omega = \Lambda_0 \supset \Lambda_1 \supset \cdots \supset \Lambda \supset \cdots \supset \Lambda_h = \{\iota\}$. By Theorem 9.7, Γ/Λ is the Galois group of K over F, and has as composition series $\Omega/\Lambda, \Lambda_1/\Lambda, \cdots, \Lambda/\Lambda = \{\iota\}$, and by Theorem 4.4 (3) of Chapter 3, the quotient groups of this composition series are isomorphic to the corresponding ones of the preceding composition series (for Ω) Hence they all are cyclic and of prime order There fore the Galois group of Λ over F is solvable ∎

(2) Let Λ be the splitting field of $f(x)$ and Γ its Galois group Let $\Gamma \supset \Gamma_1 \supset \quad \supset \Gamma_h = \{\iota\}$ be a composition series for Γ and $F = F_0 \subset F_1 \subset \quad \subset F_h = \Lambda$ be the subfields of Λ belonging to these sub groups Finally let q_1 q_2 $\quad q_h$ be the primes which are the orders of the quotient groups of the composition series By the same process used above in the latter part of the proof of (1) we can modify the chain of fields of Theorem 11 3 to get a chain of fields whose final one is C_p for $p = q_i$ $i = 1$ 2 $\quad h$ Now obviously adjoining a root of a pure equation can be done by adjoining a single radical Thus we can express the q_ith roots of unity by means of radicals Let us adjoin these to F obtaining a field N which contains C_{q_i} for $i = 1$ 2 $\quad h$ Since F_i is normal over F_{i-1} (and hence over F) and of prime degree $\exists\, \theta_i$ $i = 1$ 2 $\quad h \ni F_i = F_{i-1}(\theta_i)$ and θ_i *is a* zero of a normal poly *nomial over* F $g_i(x)$ Now either $g_i(x)$ *is reducible in* $N[x]$ *in which* case all the zeros of $g_i(x) \in N$ or $g_i(x)$ is irreducible in $N[x]$ in which case $N_i = N(\theta_i)$ is by Theorem 11 7 a pure extension and so solvable by radicals Proceding thus we reach $N(\theta_1$ θ_2 $\quad \theta_h)$ each of whose elements can be expressed in the desired manner Since $N(\theta_1$ θ_2 $\quad \theta_h) \supset \Lambda$ we have the desired result ∎

Problem 12 1 Fill in the details of the first part of the proof of (2)

Any automorphism of the splitting field of an irreducible equation $f(x) = 0$ is completely determined by specifying the images of the roots of the equation and since those images must be roots of the equation any such automorphism is determined by a mapping of the set of the roots of the equation onto itself i e by a permutation of the roots of the equation In the case of the equation $x^3 - 2 = 0$ we have found that the permutations constitute the whole symmetric group of degree 3 and order 6 In general of course the set of permutations of the roots will be a subgroup of the symmetric group of degree equal to the degree of the equation Bearing this in mind work the following exercises

Problem 12 2 Prove that every equation of degree 2 3 and 4 is solvable by radicals

Problem 12 3 Assume the following theorem The Galois group of the general equation of degree n is S_n Prove that the general equation of degree n is not solvable by radicals if $n > 4$

Chapter 7: Linear Mappings and Matrices

In this chapter we consider linear mappings of one general R-module into another. Then we consider the special case in which the R-modules are vector spaces and most of the chapter is devoted to that. In the process, matrices are introduced and various canonical forms are studied.

1. LINEAR MAPPINGS OF MODULES

Throughout this chapter, all R-modules are to be unitary unless some remark is made to the contrary, and they are to be left R-modules if R is not commutative.

DEFINITION 1.1. A homomorphism of an R-module L into (onto) an R-module M is called a *linear mapping of L into (onto) M* (cf. Definition 3.4 of Chapter 4). A linear mapping of an R-module L into itself is called a *linear transformation of L*; if it is an automorphism of L, a *nonsingular linear transformation of L*.

THEOREM 1.1. If α is a mapping of the R-module L into the R-module M, then α is a linear mapping $\Leftrightarrow \forall\ \lambda, \mu \in R, \forall\ a, b \in L$, $(\lambda a + \mu b)\alpha = \lambda(a\alpha) + \mu(b\alpha)$.

PROBLEM 1.1. Prove Theorem 1.1.

PROBLEM 1.2. Prove that if α is a linear mapping of L into M, then $\forall\ x \in L$, $\forall\ \lambda, \mu \in R$, $(\lambda\mu)(x\alpha) = \lambda(\mu(x\alpha)) = \lambda((\mu x)\alpha)$.

The product of two mappings for sets of any kind is given by Definition 1.2 of Chapter 2. The sum of two mappings can be conveniently defined only if the set in which the images lie has addition defined in it. In the piesent circumstances, we do have addition present and so we may define the sum of two linear mappings in a manner similar to that used in Definition 13.1 of Chapter 3.

DEFINITION 1.2. If α, β are linear mappings of the R-module

L into the R module M then $\alpha + \beta$ and $-\alpha$ are defined by $\forall x \in L$ $x(\alpha + \beta) = x\alpha + x\beta$ and $\forall x \in L$ $x(-\alpha) - -(x\alpha)$ Finally $\alpha - \beta$ $- \alpha + (-\beta)$

Theorem 1 2 α β are linear mappings of the R module L into the R module $M \Rightarrow \alpha + \beta$ $\alpha - \beta$ $-\alpha$ are linear mappings of L into M

Proof Let λ $\mu \in R$ a $b \in L$ Then

$$\begin{aligned}(\lambda a + \mu b)(\alpha + \beta) &= (\lambda a + \mu b)\alpha + (\lambda a + \mu b)\beta \\ &= \lambda(a\alpha) + \mu(b\alpha) + \lambda(a\beta) + \mu(b\beta) \\ &= \lambda[(a\alpha) + (a\beta)] + \mu[(b\alpha) + (b\beta)] \\ &= \lambda[a(\alpha + \beta] + \mu[b(\alpha + \beta)]\end{aligned}$$

$$\begin{aligned}(\lambda a + \mu b)(-\alpha) &= -[\lambda(a\alpha) + \mu(b\alpha)] \\ &= \lambda(-1)(a\alpha) + \mu(-1)(b\alpha) \\ &- \lambda[-(a\alpha)] + \mu[\ \ (b\alpha)] \\ &- \lambda[a(-\alpha)] + \mu[b(-\alpha)]\end{aligned}$$

That $\alpha - \beta$ is linear follows by combining the above results ■

Problem 1 3 Give a justification for each step in the above proof

Theorem 1 3 If α β γ are linear mappings of the R module L into the R module M then $\alpha + (\beta + \gamma) - (\alpha + \beta) + \gamma$

Problem 1 4 Prove Theorem 1 3

Theorem 1 4 The set E of all linear mappings of an R module L into an R module M is a group with addition as the law of composition and a left C module where C is the central of R with $r\alpha$ defined as follows $\forall r \in R$ $\forall x \in L$ $x(r\alpha) - (rx)\alpha$

Proof $x0 = 0$ is clearly a linear mapping and is the neutral element of addition Hence the first statement follows from Theorems 1 2 and 1 3

From the definition given in the theorem for $r\alpha$ we must have $\lambda[x(r\alpha)] = \lambda[r(x\alpha)] = (\lambda r)(x\alpha)$ and also $\lambda[x(r\alpha)] - (\lambda x)(r\alpha) - r[(\lambda x)\alpha] = r[\lambda(x\alpha)] - (r\lambda)(x\alpha)$ for all $\lambda \in R$ Now $(\lambda r)(x\alpha)$ will equal $(r\lambda)(x\alpha)$ for each $\lambda \in R$ only if we have $\lambda r - r\lambda$ This means that if $r \in C$ the central of R then it will be true Then we shall have $(\lambda a + \mu b)(r\alpha) - [r(\lambda a + \mu b)]\alpha - r[\lambda(a\alpha) + \mu(b\alpha)] - (r\lambda)(a\alpha) + (r\mu)(b\alpha) = r[(\lambda a)\alpha] + r[(\mu b)\alpha] - (\lambda a)(r\alpha) + (\mu b)(r\alpha) \Rightarrow r\alpha$ is linear

E is an R group since $x[(r + s)\alpha) - (r + s)(x\alpha) - r(x\alpha) + s(x\alpha) - x(r\alpha) + x(s\alpha) = x[(r\alpha) + (s\alpha)]$ so $(r + s)\alpha - (r\alpha) + (s\alpha)$

That the second condition of Definition 4 1 of Chapter 4 is satisfied follows from choosing C as the central of R ■

Corollary 1.1. E is an R-module if R is commutative.

Theorem 1.5. α is a linear mapping of an R-module L into an R-module M, β is a linear mapping of M into an R-module $N \Rightarrow \alpha\beta$ as defined in Definition 1.2 of Chapter 2 is a linear mapping of L into N.

Proof: $\forall\, \lambda, \mu \in R$, $\forall\, a, b \in L$, $(\lambda a + \mu b)(\alpha\beta) = [\lambda(a\alpha) + \mu(b\alpha)]\beta = \lambda[(a\alpha)\beta] + \mu[(b\alpha)\beta] = \lambda[a(\alpha\beta)] + \mu[b(\alpha\beta)]$. ■

Corollary 1.2. Let L, M, N, P be R-modules and α, β, γ be linear mappings of L into M, M into N, N into P, respectively. Then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ is a linear mapping of L into P.

Proof: This follows immediately from Theorem 1.1 of Chapter 2 and 1.5. ■

Corollary 1.3. The set of all linear transformations of an R-module L is a subsemigroup under multiplication of the semigroup of all mappings of L into itself.

Corollary 1.4. The set of all linear transformations of an R-module L is a ring with operators C, where C is the central of R.

Corollary 1.5. If R is a commutative ring with an identity element, the set of all linear transformations of an R-module L is an algebra over R.

Theorem 1.6. The set of all nonsingular linear transformations of an R-module L and multiplication form a group.

Problem 1.5. Prove the above four corollaries.

Problem 1.6. Prove Theorem 1.6.

Problem 1.7. Letting $x = (x_1, x_2, x_3, x_4) \in L = V_4(Q)$, $y = (y_1, y_2, y_3) \in M = V_3(Q)$, $z = (z_1, z_2, z_3) \in N = V_3(Q)$, $w = (w_1, w_2) \in P = V_2(Q)$, and α, β, γ be defined by $x\alpha = y$, where $y_1 = 3x_1 + 4x_2 - 5x_3 + 7x_4$, $y_2 = x_1 - 2x_2 + 3x_3 + x_4$, $y_3 = x_1 + x_2 + x_3 + x_4$; $y\beta = z$, where $z_1 = 4y_1 + 3y_2 - 7y_3$, $z_2 = y_1 + 2y_2 + 3y_3$, $z_3 = -2y_1 + 4y_2 + y_3$; $z\gamma = w$, where $w = z_1 + 4z_2 + 3z_3$, $w_2 = 2z_1 - 3z_2 + z_3$, prove that α, β, γ are linear mappings.

Problem 1.8. Verify Corollary 1.2 for α, β, γ of Problem 1.7.

2. MATRICES

In the case of R-modules with finite bases, linear mappings can be given in a particularly simple manner. We shall henceforth deal only with unitary R-modules with finite bases and so by Theorem 5.5 of Chapter 4, we may without loss of generality, deal with $V_n(R)$. We shall associate with each mapping a set of elements of R and this set will determine the mapping completely For this purpose we let S T U V be respectively the sets consisting of the first h m n p positive rational integers We shall further suppose that henceforth R is a commutative ring with an identity element

Theorem 2 1 The R module $R^{S\times T}$ (cf Definition 7 2 and Theorem 7 1 both of Chapter 4) and the R module E of Theorem 1 4 of all linear mappings of $V_h(R)$ into $V_m(R)$ are isomorphic

Proof Let e_1 e_2 e_h be a basis of $V_h(R)$ and f_1 f_2 f_m be a basis of $V_m(R)$ A linear mapping of $V_h(R)$ into $V_n(R)$ is of course uniquely determined by giving the images of e_1 e_h Let α be a linear mapping of $V_h(R)$ into $V_m(R)$ Then $e_i\alpha - \Sigma_{j=1}^{m} a_{ij}f_j$ $i - 1$ 2 h $a_{ij} \in R$ Thus to each such α we have an element $(a_{ij})_{i\in S\, j\in T} \in R^{S\times T}$ We shall prove that this mapping of E into $R^{S\times T}$ is an isomorphism

The mapping $\alpha \to (a_{ij})$ is determined above is onto for let $(a_{ij}) \in R^{S\times T}$ We determine an element of L whose image is (a_{ij}) as follows Let $e_i\alpha - \Sigma_{j=1} a_{ij}f_j$ for $i - 1$ 2 h This determines an image for each basis element of $V_h(R)$ Now for any element x of $V_h(R)$ $\exists$ x_1 x_2 $x_h \in R \ni x - \Sigma_{i=1}^{h} x_i e_i$ so that the image of x under α if α is to be linear must be given by $x - \Sigma_1^h x_i(e_i\alpha)$ Thus we have determined the mapping α such that under the mapping in question (a_{ij}) is the image of α

This mapping is 1 1 since if $\alpha \to (a_{ij})$ and $\beta \to (a_{ij})$ then $\forall x \in V_h(R)$ $x\alpha = x\beta$ and so $\alpha = \beta$

Now let $\alpha \leftrightarrow (a_{ij})$ $\beta \leftrightarrow (b_{ij})$ Then

$$e_i(\alpha+\beta) - e_i\alpha + e_i\beta - \sum_1^m a_{ij}f_j + \sum_1^m b_{ij}f_j - \sum_j (a_{ij}+b_{ij})f_j$$

Therefore $\alpha+\beta \leftrightarrow (a_{ij}+b_{ij}) - (a_{ij}) + (b_{ij})$

Lastly if $r \in R$ then

$$e_i(r\alpha) = r(e_i\alpha) - r\sum a_{ij}f_j - \sum^n (ra_{ij})f_j$$

and so $r\alpha \leftrightarrow (ra_{ij}) = r(a_{ij})$ ■

Problem 2 1 Verify the preservation of addition under the isomorphism of Theorem 2 1 for α of Problem 1 7 and δ given by $x\delta - y - (y_1\ y_2\ y_3)$ where $y_1 - 7x_1 + 5x_2 + 3x_3 + 5x_4$ $y_2 - x_1 + 4x_2 - 2x_3 + 7x_4$ $y_3 - 2x_1 + 2x_2 - 3x_3 - 4x_4$

Definition 2 1 Let $(a_{ij}) \in R^{S\times T}$ and $(b_{jk}) \in R^{T\times U}$ Then $(a_{ij})\ \ (b_{jk}) - (\Sigma^n{}_1\, a_{ij}b_{jk})$

THEOREM 2.2. The 1–1 mapping in the proof of Theorem 2.1 provides a 1–1 mapping of the linear mappings of $V_h(R)$ into $V_m(R)$ onto the elements of $R^{S\times T}$, those of $V_m(R)$ into $V_n(R)$ onto the elements of $R^{T\times U}$, those of $V_h(R)$ into $V_n(R)$ onto the elements of $R^{S\times U}$; further, in this 1–1 mapping to the product, in the usual sense, of a linear mapping of $V_h(R)$ into $V_m(R)$ and a linear mapping of $V_m(R)$ into $V_n(R)$ corresponds the product, in the sense of Definition 2.1, of the image elements of $R^{S\times T}$ and $R^{T\times U}$.

COROLLARY 2.1. $A \in R^{S\times T}$, $B \in R^{T\times U}$, $C \in R^{U\times V} \Rightarrow AB \in R^{S\times U}, BC \in R^{T\times V}, A(BC) + (AB)C \in R^{S\times V}$.

We leave the proof of this theorem and its corollary to the reader, but of course the method of proof is to use, as far as proving associativity is concerned, Theorem 1.1 of Chapter 2. Again we have a case in which associativity is easy to establish by relating a system to a set of mappings and using the fundamental result that the associative law holds for mappings. To prove associativity of matrices in other ways is perfectly feasible, but tedious.

THEOREM 2.3. The algebra of linear transformations of $V_h(R)$ is isomorphic to the algebra $R^{S\times S}$, with multiplication defined in Definition 2.1.

PROBLEM 2.2. Prove Theorem 2.2 and its corollary.

PROBLEM 2.3. Prove Theorem 2.3.

PROBLEM 2.4. Illustrate Corollary 2.1 with the matrices of the linear mappings α, β, γ of Problem 1.7.

DEFINITION 2.2. An element of $R^{S\times T}$ is a *matrix with elements in R* if addition and multiplication, and multiplication by elements of R are defined as in Definition 7.2 of Chapter 4 and Definitions 1.2 and 2.1. The algebra $R^{S\times S}$ of Theorem 2.3 is called the *total matric algebra over R of order* h^2, and is denoted by $\mathcal{M}_h$. The *matrix of a linear mapping* α of $V_h(R)$ into $V_m(R)$ relative to the bases (e_i) and (f_j) of $V_h(R)$ and $V_m(R)$, respectively, is the matrix corresponding to α in the isomorphism of the proof of Theorem 2.1. The *rows* of the matrix $A = (a_{ij}) \in R^{S\times T}$ are the elements $(a_{i1}, a_{i2}, \ldots, a_{im})$, $i = 1, 2, \ldots, h$ and the *columns* of the matrix $A = (a_{ij}) \in R^{S\times T}$ are the elements $(a_{1j}, a_{2j}, \ldots, a_{hj})$, $j = 1, 2, \ldots, m$, and these are often written as

Since the sets S, T, U, V are ordered sets, we shall usually take advantage of that fact and write matrices in an array which is really a double sequence

PROBLEM 2 5 Find the sum, product in both orders of

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 3 \\ -1 & 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 2 \\ -3 & 1 & 5 \\ 2 & 3 & 7 \end{pmatrix}$$

PROBLEM 2 6 Find the zero and identity elements of $\mathcal{M}_h$, the additive inverse

THEOREM 2 4 If α is a linear mapping of $V_h(R)$ into $V_m(R)$, the set of image elements is a submodule of $V_m(R)$, and the set of elements of $V_h(R)$ mapped onto 0 of $V_m(R)$ is a submodule of $V_h(R)$

PROBLEM 2 7 Prove Theorem 2 4 (Hint among other things, use theorems about homomorphisms of groups with operators)

DEFINITION 2 3 *The first submodule of Theorem 2 4 is called the range of* α *and the second the null module of* α *(null space if* R *is a field)*

3 RANK

We now suppose that R is a field F and so we deal with vector spaces (since we have previously specified that we were dealing with unitary R-modules)

DEFINITION 3 1 The *row (column) rank* of a matrix (a_{ij}) is the dimension of the space generated by the rows (columns) of (a_{ij}) The *rank (nullity)* of a linear mapping α of one vector space into another is the dimension of the range (null space) of α

PROBLEM 3 1 Find range null space rank and nullity of the mapping α of Problem 1 7

PROBLEM 3 2 Find row rank and column rank of the mapping of Problem 3 1

THEOREM 3 1 The rank of a linear mapping α of $V_h(F)$ into $V_m(F)$ is the row rank of any matrix A of α

PROOF Let $e_i\alpha = \Sigma_{j=1} a_{ij}f_j$, where $e_1 \quad , e_h$ is a basis of $V_h(F)$ and $f_1, \quad ,f_m$ is a basis of $V_m(F)$ Let the row rank of $A = (a_{ij})$ be r and suppose that $\{(a_{i1}, a_{i2} \quad , a_{im})\}_{i=1\ 2 \quad r}$ is free, renumbering the rows of A if necessary. Then the other rows of A are linearly dependent on these r rows. Let

$$(a_{b1}, a_{b2}, \ldots, a_{bm}) = c_{b1}(a_{11}, \ldots, a_{1m}) + \cdots + c_{br}(a_{r1}, \ldots, a_{rn})$$

for $b = r + 1, \ldots, h$. Then

$$\begin{aligned} c_{b1}(e_1) + \cdots + c_{br}(e_r\alpha) &= c_{b1} \sum_{j=1}^{m} a_{1j}f_j + \cdots + c_{br} \sum_{j=1}^{m} a_{rj}f_j \\ &= (c_{b1}a_{11} + \cdots + c_{br}a_{r1})f_1 + \cdots \\ &\qquad + (c_{b1}a_{1m} + \cdots + c_{br}a_{rm})f_m \\ &= a_{b1}f_1 + \cdots + a_{br}f_r = e_b\alpha, \end{aligned}$$

for $b = r + 1, \ldots, h$. Therefore, at most r of the $e_i\alpha$ are linearly independent. Therefore, rank of $\alpha \leqslant$ row rank of A.

Let the rank of α be s. Then there are s of the $e_i\alpha$ which are linearly independent while the remaining are dependent upon them. We may suppose, renumbering the e_i if necessary, that they are $e_1\alpha, \ldots, e_s\alpha$ and that for $b > s$, $e_b\alpha = d_{b1}(e_1\alpha) + \cdots + d_{bs}(e_s\alpha)$. Then we have

$$e_b = \sum_{j=1}^{m} a_{bj}f_j = d_{b1} \sum_{j=1}^{m} a_{1j}f_j + \cdots + d_{bs} \sum_{j=1}^{m} a_{sj}f_j$$

$$= (d_{b1}a_{11} + \cdots + d_{bs}a_{s1})f_1 + \cdots + (d_{b1}a_{1m} + \cdots + d_{bs}a_{sm})f_m,$$

and since the f_j are linearly independent, $a_{bj} = d_{b1}a_{1j} + \cdots + d_{bs}a_{sj}$ which implies that $(a_{b1}, \ldots, a_{bm}) = d_{b1}(a_{11}, \ldots, a_{1m}) + \cdots + d_{bs}$ $(a_{s1}, \ldots, a_{sm})$, for $s < b \leqslant h$. Hence, there are at most s linearly independent rows of A. Therefore, row rank of $A \leqslant$ rank of α. Therefore, row rank of $A =$ rank of α. ■

Problem 3.3. Verify Theorem 3.1 for α, β of Problem 1.7.

Theorem 3.2. A linear transformation α of $V_h(F)$ is nonsingular $\Leftrightarrow$ rank of $\alpha = h$.

Proof: Concerning the implication $\Longrightarrow$: Since α is an automorphism, the range of α must be $V_h(F)$ which is of dimension h, and so rank of $\alpha = h$.

Concerning the implication $\Longleftarrow$: Since the rank of α is h, the image of $V_h(F)$ is a vector subspace of $V_h(F)$ of dimension h. Then by Problem 6.4 of Chapter 4, this subspace is $V_h(F)$. Therefore, α is onto. To prove that α is 1–1, let $x, y \in V_h(F)$, $x = \Sigma_{i=1}^{h} x_ie_i$, $y = \Sigma_{i=1}^{h} y_ie_i$. Then $x\alpha = y\alpha \Longrightarrow \Sigma_{i=1}^{h} (x_i - y_i)e_i\alpha = 0$. But the $e_i\alpha$ are linearly independent, so $x_i = y_i$ and $x = y$. Therefore, α is an automorphism. ■

PROBLEM 3.4 Show that $y_1 = 3x_1 + 4x_2 - 5x_3$, $y_2 = x_1 - 2x_2 - 3x_3$, $y_3 = x_1 + x_2 + x_3$ is a nonsingular linear transformation of $V_3(Q)$.

PROBLEM 3.5 Given ϵ: $y_1 = 2x_1 + 3x_2 - 4x_3$, $y_2 = x_1 + x_2 + 2x_3$, $y_3 = 3x_1 + 4x_2 - 2x_3$, a linear transformation of $V_3(Q)$. Find its range and nullity directly, and then by using Theorem 3.1.

THEOREM 3.3 If α is a linear mapping of $V_h(F)$ into $V_m(F)$, then the rank of α plus the nullity of α = dimension of $V_h(F) = h$.

PROOF Let $\mathscr{N}$ be the null space of α, and $\mathscr{R}$ the range of α. By Problem 6.11 of Chapter 4, there exists a subspace $\mathscr{L}$ of $V_h(F)$ $\ni V_h(F)$ is the direct sum of $\mathscr{N}$ and $\mathscr{L}$. By applying Problem 6.6 of Chapter 4 we have $\dim \mathscr{N} + \dim \mathscr{L} = \dim V_h(F) = h$. So if we can show that $\mathscr{R}$ has the same dimension as $\mathscr{L}$, the theorem follows.

Each element $x \in V_h(F)$ is uniquely expressible as $x = y + z$, where $y \in \mathscr{N}$ and $z \in \mathscr{L}$. Then $x\alpha = y\alpha + z\alpha = 0 + z\alpha$, so α maps $\mathscr{L}$ into $\mathscr{R}$. If $z_1\alpha = z_2\alpha$, then $(z_1 - z_2)\alpha = 0$ and so $z_1 - z_2 \in \mathscr{N}$ and since $\mathscr{L}$ is a vector space $z_1 - z_2 \in \mathscr{L}$, and so since $\mathscr{N} \cap \mathscr{L} = \{0\}$, $z_1 = z_2$. Therefore α gives a 1–1 mapping of $\mathscr{L}$ into $\mathscr{R}$. It is obviously an onto mapping. Therefore α provides an isomorphism of $\mathscr{L}$ and $\mathscr{R}$ and so by Problem 6.7 of Chapter 4, $\mathscr{L}$ and $\mathscr{R}$ have the same dimension. ■

4 CHANGE OF BASIS

We have thus far considered linear mappings relative to a fixed basis $e_1, \ldots, e_h$ of $V_h(F)$ and a fixed basis $f_1, \ldots, f_m$ of $V_m(F)$. Now let $e_1', \ldots, e_h'$ be another basis of $V_h(F)$. Then $e_i' = \Sigma_{j=1}^{h} p_{ij} e_j$, where the $p_{ij} \in F$ since the e_j form a basis. Now since the e_i' form a basis, the e_j must be expressible in terms of the e_k', i.e. $\exists\, r_{jk} \in F \ni e_j' = \Sigma_{k=1}^{h} r_{jk} e_k$. Then combining these expressions we have

$$e_i = \sum_{j=1}^{h} p_{ij} \sum_{k=1}^{h} r_{jk} e_k = \sum_{k=1}^{h} \left(\sum_{j=1}^{h} p_{ij} r_{jk} \right) e_k$$

Now the e_i form a basis and so are linearly independent. Hence, we must have $\Sigma_{j=1}^{h} p_{ij} r_{jk} = \delta_{ik} = 1$ if $i = k$ and 0 if $i \neq k$.

PROBLEM 4.1 Prove that the matrix $I = (\delta_{ij})$, as defined above, is the neutral element of the multiplicative semigroup of Theorem 2.3.

DEFINITION 4.1 If $\{e_i\}$, $\{e_i'\}$ are bases of $V_h(F)$ and $e_i' = \Sigma_{j=1}^{h} p_{ij} e_j$, then the matrix (p_{ij}) is called the *matrix of the e_i' relative to the e_i*.

THEOREM 4.1. Let (p_{ij}) be the matrix of the basis $\{e_i\}$ of $V_h(F)$ relative to the basis $\{e_i'\}$ of $V_h(F)$ and (r_{ij}) that of $\{e_i'\}$ relative to $\{e_i\}$. Then (p_{ij}) and (r_{ij}) are matrices of nonsingular transformations and so are called *nonsingular,* and in fact are inverses of each other.

THEOREM 4.2. Let α be a linear mapping of $V_h(F)$ into $V_m(F)$, $\{e_i\}$, $\{e_i'\}$ be two bases of $V_h(F)$, with $e_i = \Sigma_{j=1}^{h} p_{ij}e_j'$, $\{f_i\}$, $\{f_i'\}$ be two bases of $V_m(F)$, with $f_k = \Sigma_{w=1}^{m} q_{kw}f_w'$, and finally let (a_{ij}) be the matrix of α relative to the bases $\{e_i\}$, $\{f_j\}$. Then the matrix of α relative to the bases $\{e_i'\}$, $\{f_j'\}$ is $(p_{ij})^{-1}(a_{ij})(q_{ij})$.

PROOF: If we let $(p_{ij})^{-1} = (r_{ij})$, we have

$$e_i'\alpha = \left(\sum_{j=1}^{h} r_{ij}e_j\right)\alpha = \sum_{j=1}^{h} r_{ij}(e_j\alpha) = \sum_{j=1}^{h} r_{ij}\sum_{k=1}^{m} a_{jk}f_k$$

$$= \sum_{j=1}^{h} r_{ij}\sum_{k=1}^{m} a_{jk}\sum_{w=1}^{m} q_{kw}f_w' = \sum_{w=1}^{m}\left(\sum_{j=1}^{h} r_{ij}\left(\sum_{k=1}^{m} a_{jk}q_{kw}\right)\right)f_w'.$$

■

COROLLARY 4.1. If $\{e_i\}$, $\{e_i'\}$ are two bases of $V_h(F)$, $e_i = \Sigma_{j=1}^{h} p_{ij}e_j'$, and if α is a linear transformation of $V_h(F)$ with matrix (a_{ij}) relative to $\{e_i\}$, then α has matrix $(p_{ij})^{-1}(a_{ij})(p_{ij})$ relative to $\{e_i'\}$.

PROBLEM 4.2. Considering the linear mapping α of Problem 1.7 as relative to $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$ as a basis of $V_4(Q)$ and $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ as a basis of $V_3(Q)$, find the matrix of this mapping relative to $(1,1,0,0)$, $(1,0,1,0)$, $(1,0,0,1)$, $(0,0,1,1)$ as a basis of $V_4(Q)$ and $(1,1,1)$, $(0,1,1)$, $(1,0,1)$ as a basis of $V_3(Q)$.

PROBLEM 4.3. Considering the linear mapping β of Problem 1.7 as a linear transformation of $V_3(Q)$ relative to $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, find the matrix of β relative to $(1,1,1)$, $(0,1,1)$, $(1,0,1)$.

PROBLEM 4.4. Prove the product of two nonsingular matrices is nonsingular.

5. COORDINATES

DEFINITION 5.1. If $e_1, e_2, \ldots, e_h$ is a basis of $V_h(R)$, where R is a ring, if $x \in V_h(R)$, and if $x = \Sigma_{i=1}^{h} x_ie_i$, then $x_1, x_2, \ldots, x_h$ are the *coordinates of x relative to (or with respect to) the basis* $\{e_i\}$.

THEOREM 5.1. If $\{e_i\}$, $\{f_j\}$ are bases of $V_h(R)$ and $V_m(R)$, respectively, R a ring, if α is a linear mapping of $V_h(R)$ into $V_m(R)$

with matrix (a_{ij}), then $x \in V_h(R)$ is mapped onto $y \in V_h(R)$ where $y_j = \sum_{i=1}^{l} x_i a_{ij}$, $j = 1, 2, \quad , m$, and $y = (y_1, y_2 \quad , y_m)$, and where $x_1, x_2, \quad , x_h$ and $y_1, y_2, \quad , y_m$ are, respectively, the coordinates of x and y

Proof $x \in V_h(R) \Rightarrow x = \sum_{i=1}^{h} x_i e_i$, $x_i \in R$ Then

$$y = x\alpha = \left(\sum_{i=1}^{l} x_i e_i\right)\alpha = \sum_{i=1}^{h} x_i(e_i\alpha)\Big) = \sum_{i=1}^{h} x_i \sum_{j=1}^{m} a_{ij} f_j$$

$$= \sum_{j=1}^{m}\left(\sum_{i=1}^{h} x_i a_{ij}\right) f_j \Rightarrow y_j = \sum_{i=1}^{h} x_i a_{ij}$$ ■

Corollary 5 1 Each $y \in V_m(R)$, and $y \in$ range of α is a linear combination of the rows of the matrix (a_{ij})

Corollary 5 2 The rank of the linear mapping α is equal to the row rank of the matrix (a_{ij}) *of* α

Corollary 5 3 The equations $\sum_{i=1}^{h} x_i a_{ij} = 0$, $j = 1\ 2, \quad , m$ always have solutions other than $(0\ 0 \quad 0)$ if $h > m$

Problem 5 1 Prove Corollaries 5 1 and 5 2

Problem 5 2 Use Theorem 3 3 to prove Corollary 5 3

Theorem 5 2 For a linear mapping α of $V_h(F)$ into $V_m(F)$, where F is a field $\exists$ bases of $V_h(F)$ and $V_m(\Gamma)$ $\ni$ relative to these bases, α has matrix

$$\begin{array}{c} \overbrace{\hphantom{1 \quad 0 \qquad\quad 0}}^{r} \hphantom{\quad 0 \qquad\quad 0} \\ \begin{pmatrix} 1 & 0 & & 0 & 0 & & 0 \\ 0 & 1 & & 0 & 0 & & 0 \\ & & & & & & \\ 0 & 0 & & 1 & 0 & & 0 \\ 0 & & & 0 & 0 & & 0 \\ & & & & & & \\ 0 & & & & & & 0 \end{pmatrix} \end{array}$$

where r is the rank of α

Proof Let $y_1, \quad y_s$ be a basis for the null space of α Then $\exists\, x_1, \quad x_r \ni x_1, \quad x_r, y_1, \quad y_s$ form a basis of $V_h(F)$, and $r + s = h$ Since $y_i\alpha = 0$, $x_i\alpha$ are generators of the range of α and so are clearly linearly independent since the rank of α is r Let $u_i = x_i\alpha$ and $v_i \in V_m(F)$ and be such that $u_1, \quad , u_r\ v_1, \quad , v_{m-r}$ form a basis of $V_m(F)$ Then we have $x_i\alpha = u_i$, for $i = 1, 2, \quad , r$ and $y_i\alpha = 0$, for $i = 1, 2, \ldots, h - r$, and so the matrix of α is as described in the theorem. ∎

6. APPLICATION TO LINEAR EQUATIONS

We shall apply the material of the last paragraph to considering the solutions of systems of linear equations.

DEFINITION 6.1. $c \in V_h(F)$, where F is a field, is a *solution* of the equation $\Sigma_{i=1}^{h} x_i a_i = d$, where $d, a_i \in F \Leftrightarrow \Sigma_{i=1}^{h} c_i a_i = d$. If $d = 0$, the equation is called *homogeneous*; if $d \neq 0$, *nonhomogeneous*.

THEOREM 6.1. The set of all vectors of $V_h(F)$, each of which is a solution of $\Sigma_{i=1}^{h} x_i a_{ij} = 0$, $a_{ij} \in F$, $j = 1, 2, \ldots, m$, is a subspace of $V_h(F)$. The dimension of this subspace is $h - r$, where r is the row rank of $A = (a_{ij})$. In particular, there will always be at least one solution, not $(0, 0, \ldots, 0)$, if $h > m$. We shall call this set of equations a *homogeneous* system of equations and denote it by (H).

PROOF: Let $e_1, \ldots, e_h$ be a basis of $V_h(F)$, $f_1, \ldots, f_m$ be a basis of $V_m(F)$, and α be the linear mapping of $V_h(F)$ into $V_m(F)$ defined as in the proof of Theorem 5.1, by $x\alpha = y_1 f_1 + \cdots + y_m f_m$ where $y_j = \Sigma_{i=1}^{h} x_i a_{ij}$, $j = 1, 2, \ldots, m$. Then the set of solutions of the system (H) is the null space of α and by Theorem 2.4, it is a subspace of $V_h(F)$. That its dimension is $h - r$ follows immediately from Theorems 3.1 and 3.3. Obviously, the row rank of A cannot be greater than m, so if $h > m$, $h - r > 0$, and so there exists nonzero elements of $V_h(F)$ which satisfy (H). ∎

PROBLEM 6.1. Prove that the range of a linear mapping α of $V_h(F)$ into $V_m(F)$ is generated by the rows of the matrix of α.

THEOREM 6.2. The system of equations, (N) $\Sigma_{i=1}^{h} x_i a_{ij} = d_j$, $a_{ij}, d_j \in F$, has a solution $\Leftrightarrow$ the row rank of $A = (a_{ij})$ is equal to the row rank of

$$B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ & & \cdots & \\ a_{h1} & a_{h2} & \cdots & a_{hm} \\ d_1 & d_2 & \cdots & d_h \end{pmatrix}.$$

If $(t_1, t_2, \ldots, t_h)$ is a solution of (N) and $(z_1, z_2, \ldots, z_h)$ is a solution of (H), then $(t_1, t_2, \ldots, t_h) + (z_1, z_2, \ldots, z_h)$ is a solution of (N); furthermore, every solution of (N) can be represented in this form for a fixed $(t_1, t_2, \ldots, t_h)$ by a suitable choice of $(z_1, z_2, \ldots, z_h)$.

PROBLEM 6.2. Prove Theorem 6.2.

PROBLEM 6.3. (a) With $A = \begin{pmatrix} 2 & 3 & -4 \\ 1 & 4 & 5 \\ 3 & 7 & 1 \end{pmatrix}$ solve (H).

(b) with the same A and $d_1 = 4$, $d_2 = 11$, $d_3 = 6$, solve (N).

(c) with the same A, and $d_1 = 3$, $d_2 = 7$, $d_3 = 2$, solve (N).

COROLLARY 6.1. If α is a nonsingular transformation of $V_h(F)$ with matrix $A = (a_{ij})$, the system (N) has one and only one solution.

PROBLEM 6.4. Without using Theorem 6.2 prove Corollary 6.1.

7. ROW EQUIVALENCE AND ELEMENTARY OPERATIONS

Here R is a ring with an identity element.

DEFINITION 7.1. (a) A is an $h \times m$ matrix $\Leftrightarrow A \in R^{S \times T}$ where $S = \{1, 2, \ldots, h\}$, $T = \{1, 2, \ldots, m\}$.

(b) Let A and B be $h \times m$ matrices. Then A is *row (column) equivalent* to $B \Leftrightarrow$ the module generated by the rows (columns) of A is the same as the module generated by the rows (columns) of B. If R is a field, the modules will be the row space or the column space.

DEFINITION 7.2. Let $A \in R^{S \times T}$. An *elementary row (column) operation* performed on A is any one of the following:

(a) the interchange of two rows (columns);

(b) the multiplication of a row (column) by a unit of R;

(c) the addition to the elements of any row (column) of A of λ times the corresponding elements of any other (definitely not the same) row (column), where $\lambda \in R$.

THEOREM 7.1. If any elementary row (column) operation is performed on a matrix A, the resulting matrix is row (column) equivalent to A, and if R is a field the resulting matrix has the same row (column) rank as A.

PROOF. The conclusion of the theorem is obvious if the elementary operation is of type (a) or (b). We shall consider the case of an elementary operation of type (c). Let $r_1, r_2, \ldots, r_h$ be the rows of A and let c be the element of R by which we multiply, say, the first row and add the results to the corresponding elements of the second row. (There is no restriction on the generality by choosing these two rows, and it makes the notation much simpler.) If x is in the module generated by the original rows, then it can be expressed in the form $a_1r_1 + a_2r_a + \cdots + a_hr_h = x$, but we may write this as $x = (a_1 - a_2c)r_1 + a_2(r_2 + cr_1) + \cdots + a_hr_h$, where the $a_i \in R$, but this latter expresses x as in the module generated by the new rows. On the other hand, if x is in the module generated by the new rows, then $x = b_1r_1 + b_2(r_2 + cr_1) + \cdots + b_hr_h$, where the $b_j \in R$. But this can be written as $x = (b_1 + b_2c)r_1 + b_2r_2 + \cdots + b_hr_h$ which shows that if x is in the module generated by the new rows, it is in the module generated by the original rows. Therefore, the two modules are the same and so the two matrices are row equivalent. Exactly similar reasoning applies to the case of operations with columns. The statement about the case in which R is a field follows from the definition of row and column rank. ■

THEOREM 7.2. Row (column) equivalence is an equivalence relation.

PROBLEM 7.1. Prove Theorem 7.2.

DEFINITION 7.3. Let $A, B \in R^{S \times T}$. Then A is *equivalent to B* $\Leftrightarrow$ B can be obtained from A by a finite number of elementary row and column operations.

THEOREM 7.3. Equivalence of matrices is an equivalence relation.

PROBLEM 7.2. Prove Theorem 7.3.

THEOREM 7.4. The matrix $I_h = (\delta_{ij})$, where $\delta_{ij} = 0$ for $i \neq j$, $\delta_{ii} = 1$, is the identity element for $\mathcal{M}_h$. Further, $I_hA(AI_h) = A$ for any $h \times n(m \times h)$ matrix A. (When, from the context, it is clear what the size of I_h must be, we shall often omit the subscript.)

DEFINITION 7.4. An *elementary matrix* is any matrix obtained from the identity matrix by performing *exactly one* elementary row or column operation.

THEOREM 7.5. An elementary matrix is nonsingular.

PROBLEM 7.3. Prove Theorem 7.4.

PROBLEM 7.4. Prove Theorem 7.5. (Hint: use Theorem 7.1.)

PROBLEM 7.5. Write an elementary 3 × 3 matrix of each of the possible types of Definition 7.2. Do this for both row and column operations.

PROBLEM 7 6 Show that any elementary matrix may be obtained by either an elementary row operation or an elementary column operation

PROBLEM 7 7 Prove that an elementary row (column) operation performed on a matrix A can be performed by multiplying A on the left (right) by the elementary matrix obtained by performing on the identity matrix the given elementary row (column) operation

PROBLEM 7 8 Verify the statement of Problem 7 7 for the matrix $A = \begin{pmatrix} 2 & 4 & 5 \\ -1 & 3 & 7 \\ 4 & 0 & 1 \end{pmatrix}$

PROBLEM 7 9 Prove that the product of any finite number of elementary matrices is nonsingular

THEOREM 7 6 If the matrix A is row (column) equivalent to the matrix B then $B = PA$ ($B = AQ$) where $P(Q)$ is nonsingular and further is the product of elementary matrices

PROBLEM 7 10 Prove Theorem 7 6 (Hint use Definition 7 1 the method of the proof of Theorem 7 1 and Problem 7 7)

COROLLARY 7 1 If the matrix A is equivalent to the matrix A then there exist nonsingular matrices P and Q such that $PAQ = B$

We have in this present section been considering matrices with elements in in arbitrary ring R We shall very soon consider matrices with elements in a field F but first for convenience we establish some further results about vector subspaces

8 A PARTICULAR KIND OF BASIS FOR A VECTOR SUBSPACE

We first prove a lemma

LEMMA If the vector space S over F is generated by a_1 a a_k then S is generated by a_1 $a_{\ 1}$ b a a_k where $b_i - \sum_{=1}^{k} \lambda_j a_j$ $\lambda \in F$ $\lambda \neq 0$ for each $i - 1$ 2 k

PROOF Obviously the vector space generated by the second set of vectors is contained in S Now

$$a_i - -\frac{\lambda_1}{\lambda} a_1 - \qquad -\frac{\lambda_{\ 1}}{\lambda_i} a_{\ 1} + \frac{1}{\lambda_i} b \quad \frac{\lambda_{\ 1}}{\lambda_i} a_{+1} - \qquad \frac{\lambda_k}{\lambda} a_k$$

Thus every vector in S can be expressed as a linear combination of the vectors of the second set. Therefore, the two spaces are the same. ■

The proof of the next Theorem is not particularly difficult, but it is slightly tedious. The reader would be well advised to take some particular matrix and carry through each step of the proof with it.

THEOREM 8.1. Let the vector subspace $S \subset V_h(F)$ be generated by $a_i = (a_{i1}, \ldots, a_{ih}), j = 1, 2, \ldots, k$. Then S has a basis $(b_{i1}, b_{i2}, \ldots, u_{ih}) = b_i$, $i = 1, 2, \ldots, m$, such that there exists a strictly increasing finite sequence j_i (i.e., $j_i < j_p$ for $i < p$), (1) $b_{ij} = 0$ if $j < j_i$; (2) $b_{ij_i} = 1$; (3) $b_{uj_i} = 0$, for $u \neq i$.

PROOF: If any of the a_{i1} are different from zero, let $j_1 = 1$. Otherwise, let j_1 be the smallest j such that for some i, $a_{ij} \neq 0$. Then among the a_{ij_1} which are not zero, let $a_{i_1j_1}$ be that one with smallest i. Now let $c_{1j} = (1/a_{i_1j_1})\, a_{i_1j}$, $j = 1, \ldots, h$. Then by the above lemma, S is generated by the set of vectors obtained by replacing a_{i_1} by $c_1 = (c_{11}, c_{12}, \ldots, c_{1h})$ in the original set. Let us now remember, if necessary, the original set of the a_i so that a_{i_1} becomes a_1. Then S is generated by $c_1, a_2, \ldots, a_k$ and we have $c_{1j} = 0$ for $j < j_1$; $a_{ij} = 0$ for $j < j_1$; $c_{ij_1} = 1$.

Now replace each $a_i i > 1$, by $a_i - a_{ij_1}c_1 = c_i$. Then $c_1, c_2, \ldots, c_k$ generate S, by the lemma, and $c_{ij} = 0$ for $j \leqslant j_1$, $i > 1$. Now, if $j_1 < h$, on operating on $c_2, \ldots, c_k$ in the same manner, we get a set $c_1 d_2, \ldots, d_k$ such that these k vectors generate S and $d_{ij} = 0$ for $k \leqslant j_2$, $i > 2$; $d_{2j_2} = 1$. Now replace c_1 by $d_1 = c_1 - c_{1j_2}d_2$ and we have further that $d_{1j_2} = 0$.

Continuing by induction, we finally reach a set of vectors $e_1, \ldots, e_k$ which generate S and have the properties: $e_{ij} = 0$ if $j < j_1$, $e_{ij_i} = 1$, $e_{vj_i} = 0$, if $v < i$, and further $e_1, e_2, \ldots, e_r$ generate S.

Now we replace $e_1, \ldots, e_r$ by $b_i = e_i - e_{ij_r}e_r$, for $i < r$ and $b_r = e_r$, and we have a set of vectors which possess the properties stated in the theorem. That they generate S is clear from their derivation with frequent use of the lemma. That they are linearly independent follows immediately from the three properties. Therefore, they are a basis of S. ■

PROBLEM 8.1. Verify in detail the linear independence of the b_i.

PROBLEM 8.2. Find a basis of the type of Theorem 8.1 for the vector space generated by $a_1 = (0, 0, 0, 3, 2, 4)$, $a_2 = (0, 0, 0, 4, 2, 0)$, $a_3 = (0, 0, 0, 0, 3, 1)$.

PROBLEM 8 3 Do the same as in Problem 8 2 for $a_1 = (1\ 3\ 5\ 2\ -1)$ $a = (3\ 4\ 2\ -2\ 3)$ $a_3 - (4\ 2\ 1\ 5\ 3)$ $a_4 = (8\ 9\ 8\ 5\ 5)$

9 EQUIVAI ENCE OF MATRICES OVER A FIELD

We now consider matrices with elements in a field F and we shall find that m iny of the theorems of Section 7 ire such that their converses also hold

THEOREM 9 1 The matrix A is row (column) equivalent to the matrix $B \Rightarrow A$ and B have the s ime row (column) rank

PROBLEM 9 1 Prove Theorem 9 1

THEOREM 9 2 The $h \times m$ m itrix A h is row rank $r \Rightarrow A$ is row equivalent to a matrix of the form

$$\left.\begin{pmatrix} 0 & 0 & & a_{1j_1} & a & 0 & a_{1\cdot} & a & & a_{1\cdot} & & 0 & a_{1j} & a_{1m} \\ 0 & 0 & 0 & 0 & 0 & a_{2j_2} & a & a_{2\cdot} & 0 & a_{2j} & a_{2j} & 0 & a_{2j} & a_{2m} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a & a & 0 & a_{3j_r} & a_{3m} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & a_{rj} & a_{rm} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}\right\} h$$

where $a_{ij} - 1$

PROBLEM 9 ? Use Theorem 8 1 to prove Theorem 9 ?

PROBLEM 9 3 Give the form for column equivalence corresponding to the form of Theorem 9 2

PROBLEM 9 4 Find a matrix of the form of Theorem 9 2 row equivalent to

$$A - \begin{pmatrix} 2 & 1 & -4 & 1 \\ -2 & -1 & 4 & 1 \\ 2 & 2 & 4 & 3 \\ 10 & 7 & -4 & 9 \end{pmatrix}$$

THEOREM 9 3 (cf Problem 7 9) A matrix over a field F is nonsingular $\Leftrightarrow A$ is a product of elementary matrices

PROOF The implication $\Leftarrow$ is established by Problem 7 9

The implication $\Rightarrow$ If $A \in \mathcal{M}_h$ is nonsingular it is of row rank h and so by Theorem 9 2 row equivalent to the identity matrix I Thus by Theorem 7 6 $I - PA$ where P is a product of a finite number of elementary matrices Letting $P - E_1 E \qquad E_k$ we have $A = E_k{}^{1} E_{k\ 1} \qquad E_2{}^{1} E_1{}^{1}$ ■

COROLLARY 9.1. If $B = PA$ $(B = AQ)$ where $P(Q)$ is nonsingular, then B is row (column) equivalent to A.

PROBLEM 9.5. By using the method of the proof of Theorem 9.3, find the inverse of $\begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 3 \\ -1 & 2 & 3 \end{pmatrix}$.

PROBLEM 9.6. Prove Corollary 9.1.

THEOREM 9.4. A is row (column) equivalent to $B \Rightarrow$ column (row) rank of A = column (row) rank of B.

PROOF: By Theorems 3.1 and 3.3, if we can show that the null space of B is the same as the null space of A, we have the theorem. (We shall prove the parenthetical statement.)

Since A and B are column equivalent, there exists a nonsingular Q such that $B = AQ$. Let σ be the nonsingular linear transformation with matrix Q, and α and β the linear mappings with matrices A, B, respectively. Then $\beta = \alpha\sigma$.

Now if $x \in$ null space of α, then $x\alpha = 0$, and so $x\beta = x(\alpha\sigma) = (x\alpha)\sigma = 0\sigma = 0$, and so the null space of $A \subset$ null space of B.

On the other hand, if $x \in$ null space of B, then $x\beta = 0$. Then we have $x\alpha = (x\alpha)(\sigma\sigma^{-1}) = x(\alpha\sigma)\sigma^{-1} = (x\beta)\sigma^{-1} = 0\sigma^{-1} = 0$, and so the null space of $B \subset$ null space of A.

Therefore, null space of B = null space of A. ■

PROBLEM 9.7. Prove the other case of Theorem 9.4.

THEOREM 9.5. The matrix A over the field F is of row rank $r \Rightarrow A$ is equivalent to the matrix (c_{ij}), where $c_{ij} = 0$ for $i \neq j$, $c_{ii} = 1$ for $i < r$, and $c_{ii} = 0$ for $i > r$.

PROOF: By elementary row operations, A is equivalent to a matrix of the form given in Theorem 9.2. Then by elementary column operations of type 3, all the nonzero elements except the a_{ij_i} can be eliminated. Then by further elementary operations, this time of type 1, the a_{ij_i} can be moved to the position specified in the theorem. ■

THEOREM 9.6. If A is a matrix over a field F, then row rank of A = column rank of A.

PROOF: Let A' be the matrix, row equivalent to A, obtained by the use of Theorem 9.2 and A'' that obtained from A' by the use of Theorem 9.5. By these two theorems, A and A'' have the same row rank. Now, since A is row equivalent to A', by Theorem 9.4, the column rank of A = column rank of A'. Now the process used in the proof of Theorem 9.5 to obtain A'' from A' consisted of using only elementary column operations and so A'' has the same column rank as A' and the same column rank as A. Now A'' has obviously the same row rank as column rank. Therefore the column rank of A = row rank of A. ■

After Theorem 9.6 we are justified in making the following definition for matrices with elements in a field.

Definition 9.1 If A is a matrix over a field, then the *rank of A* is its row rank.

Theorem 9.7 Two matrices over a field F are equivalent if and only if they have the same rank.

Problem 9.8 Prove Theorem 9.7.

10 EQUIVALENCE OF MATRICES OVER A EUCLIDEAN RING

Much of what we have established about matrices over a field can be applied to matrices over a Euclidean ring. To facilitate this application, we prove the following lemma.

Lemma Let R be an integral domain and F its field of quotients and let $x_1, x_2, \ldots, x_k \in V_n(R)$. Then $x_1, x_2, \ldots, x_k$ are linearly independent elements of $V_n(R) \Leftrightarrow x_1, x_2, \ldots, x_k$ are linearly independent elements of $V_n(F)$.

Proof The implication $\Leftarrow$ is obvious.

The implication $\Rightarrow$. Suppose that $x_1, x_2, \ldots, x_k$ are linearly independent in $V_n(R)$ but not in $V_n(F)$. Then $\exists\, a_i \in F$, not all $0 \ni \sum_{i=1}^{k} a_i x_i = 0$. Now let $a_i = b_i/c_i$ where $b_i, c_i \in R$, and let d be the product of all the c_i for which $b_i \neq 0$. Then $da_i \in R\ \forall i$, and we have $\sum_{i=1}^{k} da_i x_i = 0$, where the coefficients $\in R$ and are not all zero since the a_i are not all zero. We have a contradiction and so the $x_1, x_2, \ldots, x_k$ are linearly independent in $V_n(F)$. ■

In Definition 9.1 we defined the row rank of a matrix over a field. Because of the above lemma, we are justified in making the following definition for matrices over an integral domain.

Definition 10.1 The row rank, column rank, and rank of a matrix A over an integral domain I is the appropriate rank of A considered as a matrix over F, the field of quotients of I.

For matrices over a field we had the very convenient result given by Theorem 9.7, that if two matrices have the same rank they are equivalent. This is no longer true when we consider matrices over an integral domain as Problem 10.1 below show. First, we need a definition.

DEFINITION 10.2. A matrix $A = (a_{ij})$ is called a *diagonal matrix* $\Leftrightarrow \forall\, i \neq j$, $a_{ij} = 0$. Such a matrix is denoted by diag$(a_{11}, a_{22}, \ldots, a_{hh})$.

PROBLEM 10.1. Prove that diag$(1, 1, 1) = A$ and diag$(2, 2, 2) = B$ are equivalent as matrices over Q but not as matrices over Z.

THEOREM 10.1. Let E be a Euclidean ring. Then a matrix $A = (a_{ij})$ of rank r, considered as a matrix over E, is equivalent to a matrix diag$(h_1, h_2, \ldots, h_r, 0, 0, \ldots, 0)$, where $h_i | h_{i+1}$, for $i = 1, 2, \ldots, r-1$; $h_i \neq 0$ for $i = 1, 2, \ldots, r$.

PROOF: Consider $\delta(a_{i1})$, $i = 1, 2, \ldots, k$, where $\delta(x)$ is given in Definition 4.1 of Chapter 5. If $\delta(a_{11})$ is not the smallest positive integer in this set, bring the smallest one into position $(1, 1)$, by interchanging rows. Then, since $\exists\, q_i, r_i \in R \ni a_{i1} = a_{11}q_i + r_i$ (using now the new a_{11}), where $\delta(r_1) < \delta(a_{11})$, by multiplying the first row by $-q_i$ and adding it to the ith, if $\delta(r_i) > 0$, we get in the position $(i, 1)$, r_i. If not all $\delta(r_i)$, $i > 1$, are zero, let $\delta(r_j)$ be the smallest positive $\delta(r_i)$, $i \geqslant 1$. Then we can move it to position $(1, 1)$ (if it is not already there), and continue. Finally, since δ is integral valued, we get zeros in the first column below the position $(1, 1)$. Now, if $\delta(a_{11})$ is the minimum positive value among the $\delta(a_{1j})$, we can proceed for the first row as we did for the first column and get zeros to the right of the position $(1, 1)$. If not, replace a_{11} by that element in the first row with minimum positive δ value. Then, as before for the first column, we can get zeros in all the places of the first row. Now, in this process we may have introduced some nonzero elements in the positions $(i, 1)$ for $i > 1$. But, we have now in the $(1, 1)$ position an element of smaller positive δ value than before. By continuing the process, since δ takes on only nonnegative integral values, we eventually get a matrix equivalent to the original one with zeros in the first column and the first row except in position $(1, 1)$.

Of course, if all the elements in the first column are zero, we may by an elementary operation bring, if $A \neq 0$, (of course, if $A = 0$ the theorem is trivially true) a nonzero element into position $(1, 1)$.

Now we proceed in like manner to get in the position $(2, 2)$ a nonzero element if there is one left in the matrix besides that in position (1 1) and we proceed to get zeros in the second row and second column except for position (2 2) In the process the first row and first column are not affected and have no effect upon any of the other rows

Continuing thus we get a diagonal matrix $\operatorname{diag}(d_1\ d_2\ \ldots\ d_r\ 0\ \ldots\ 0)$ If $d_i | d_{i+1}$ we are through If not by elementary operations we may move the d_i of smallest δ value into position (1 1) Then if $d_1 \nmid d_2$ we may multiply the first row by $-q$ where $d_2 = d_1 q + s$ $\delta(s) < \delta(d_1)$ and then add the first column to the second column Then multiply the first row by q and add to the second and we have $\operatorname{diag}(d_1\ s\ d_3\ \ldots)$ Now interchange as before s and d_1 Continuing thus we eventually get $\operatorname{diag}(h_1\ \ldots\ h_r\ 0\ \ldots\ 0)$ where $h_i | h_{i+1}$ $i = 1\ 2\ \ldots\ r-1$

It follows from considering the field of quotients F of E and then applying Theorem 9 5 that exactly r of the h_i are not zero ∎

The form of the matrix in Theorem 10 1 is called the *Smith normal form*

Problem 10 2 Apply Theorem 10 1 to $\begin{pmatrix} 2 & 4 \\ 6 & 8 \end{pmatrix}$ as a matrix over Z

Problem 10 3 Apply Theorem 10 1 to $\begin{pmatrix} \lambda & \lambda & 0 \\ \lambda & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix}$ as a matrix over $Q[\lambda]$

11 EQUIVALENCE OVER $F[\lambda]$ SIMILARITY

We are now going to apply some of the results about equivalence of matrices over a Euclidean domain to a particular Euclidean domain $F[\lambda]$ where F is a field and λ an indeterminate Then we shall apply these to another kind of equivalence relation in $\mathcal{M}_h$

We shall now use Λ as an indeterminate when we have matrices as coefficients and λ as an indeterminate when we have elements of F as coefficients Thus $R^{s\times s}[\Lambda]$ is the set of all polynomials in Λ with coefficients $h \times h$ matrices with elements in R while $(R[\lambda])^{s\times s}$ is the set of all $h \times h$ matrices whose elements are polynomials in λ with coefficients in R

Theorem 11 1 If R is a commutative ring with an identity element then as algebras over R $R^{s\times s}[\Lambda]$ is isomorphic to $(R[\lambda])^{s\times s}$

PROBLEM 11.1. Prove Theorem 11.1.

We now need a definition and a proposition about polynomials for which we have had no previous need.

DEFINITION 11.1. If the leading coefficient of $f(x)$, of degree n, $\in R[x]$, where R is a ring, is a unit of R, then $f(x)$ is said to be *proper of degree n* or *of proper degree n*.

LEMMA. Let $a(x)$, $b(x) \in R[x]$, where R is a ring with an identity element, and a, b are proper of degrees m_2 and m_1, respectively. Then if $a(x)p_1(x) = p_2(x)b(x)$, where $p_1(x)$, $p_2(x) \in R[x]$, $\exists\, q(x)$, $r_1(x)$, $r_2(x) \in R[x] \ni r_i(x) = 0$ or deg $r_i(x) < m_i$, for $i = 1, 2$ and such that

$$a(x)r_1(x) = r_2(x)b(x),$$
$$p_1(x) = q(x)b(x) + r_1(x),$$
$$p_2(x) = a(x)q(x) + r_2(x).$$

PROOF: By Theorem 1.4 of Chapter 5, $\exists\, q_1, q_2, r_1, r_2 \in R[x]$ $\ni r_i = 0$ or deg $r_i < m_i$ for $i = 1, 2$ and $p_1(x) = b(x)q_1(x) + r_1(x)$, $p_2(x) = a(x)q_2(x) + r_2(x)$. Then $ar_1 - r_2b = ap_1 - aq_1b - p_2b + aq_2b$ $= aq_2b - aq_1b = a(q_2 - q_1)b$. Now $ar_1 - r_2b$ is either zero or, by Theorem 1.3 of Chapter 5, of degree $< m_1 + m_2$. Since a unit is a regular element, $a(q_2 - q_1)b$ is either 0 or of degree $\geqslant m_1 + m_2$. Therefore, both these expressions are 0, and we have $ar_1 = r_2b$, and $q_1 = q_2 = q$. ■

THEOREM 11.2. If A and B are equivalent matrices of $(F[\lambda])^{S\times S}$, and if the corresponding elements of $F^{S\times S}[\Lambda]$, given by Theorem 11.1, are proper of degree 1, then there exists nonsingular matrices P, Q $\in F^{S\times S} \ni A = PBQ$, where F is a field.

PROOF: Since A and B are equivalent, $\exists\, P_1, P_2 \in (F[\lambda])^{S\times S}$, products of elementary matrices, $\ni AP_1 = P_2B$. The corresponding elements of $F^{S\times S}[\Lambda]$ can, without serious confusion, be denoted by the same letters. Since A and B (as elements of $F^{S\times S}[\Lambda]$) are of degree 1, by the above lemma, $\exists\, R_1, R_2 \in F^{S\times S} \ni AR_1 = R_2B$. If we can establish that R_1 and R_2 are nonsingular, the desired result easily follows. Let us apply Theorem 1.4 of Chapter 5 to P_1^{-1} (P_1^{-1} exists and $\in F^{S\times S}[\Lambda]$ by Theorem 7.6), and we have $P_1^{-1} = Q_3A + R_3$, where $R_3 = 0$ or deg $R_3 = 0$. Also, by the lemma, $\exists\, Q$, $\ni P_1 = QB + R_1$. where $R_1 = 0$ or deg $R_1 = 0$. Then we have $I = P_1^{-1}P_1 =$ $(Q_3A + R_3)(QB + R_1) = Q_3AQB + Q_3AR_1 + R_3QB + R_3R_1$ and so $I - R_3R_1 = Q_3AQB + Q_3R_2B + R_3QB$. The left side of this last equation is either 0 or of degree 0 while the right side equals $(Q_3AQ + Q_3R_2 + R_3Q)B$ and so is 0 or of degree $\geqslant 1$ since B is proper of degree 1. Therefore, both sides are 0, i.e. $R_3R_1 = I$ and so R_1 is nonsingular since it has an inverse R_3. Similarly, R_2 is nonsingular. Then $A = R_2BR_1^{-1}$ or $A = PBQ$, where $P = R_2$ and $Q = R_1^{-1}$. ∎

Theorem 11.3 Two $h \times m$ matrices, with elements in a field F, are equivalent $\Leftrightarrow$ they are matrices of the same linear mapping of $V_h(F)$ into $V_m(F)$ for suitably chosen bases of $V_h(F)$ and $V_m(F)$.

Problem 11.2 Prove Theorem 11.3. (Hint: use Theorem 4.2 and Corollary 7.1.)

Definition 11.2 Two matrices A and B are *similar* $\Leftrightarrow \exists$ a nonsingular matrix $P \ni A = P^{-1}BP$.

Theorem 11.4 Similarity of matrices is an equivalence relation.

Theorem 11.5 Two matrices are similar $\Leftrightarrow$ they are matrices of the same linear transformation with respect to suitably chosen bases.

Problem 11.3 Prove Theorem 11.4.

Problem 11.4 Prove Theorem 11.5.

Theorem 11.6 $A, B \in F^{s\times s}$ are similar $\Leftrightarrow \lambda I - A, \lambda I - B \in (F[\lambda])^{s\times s}$ are equivalent.

Proof The relation $\Rightarrow$. Let $A = P^{-1}BP$. Then $\lambda I - A = \lambda I - P^{-1}BP = P^{-1}(\lambda I - B)P \Rightarrow \lambda I - A$ and $\lambda I - B$ are equivalent.

The relation $\Leftarrow$. Let $\lambda I - A$ and $\lambda I - B$ be equivalent. Then by Theorem 11.2 there exist nonsingular matrices $P, Q \in F^{s\times s} \ni P(\lambda I - B)Q = \lambda I - A = \lambda PQ - PBQ \Rightarrow PQ = I \Rightarrow A = Q^{-1}BQ \Rightarrow A, B$ are similar. ∎

12. VECTOR SUBSPACES INVARIANT UNDER A LINEAR TRANSFORMATION

First we make a remark about notation. For brevity, we sometimes write a matrix as a matrix of blocks. Thus instead of

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & a_{1\,n+1} & \cdots & a_{1m} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} & a_{k\,n+1} & \cdots & a_{km} \\ 0 & \cdots & 0 & a_{k+1\,n+1} & \cdots & a_{k+1\,m} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{r\,n+1} & \cdots & a_{rn} \end{pmatrix}$$

we write $\begin{pmatrix} A_1 & A_3 \\ 0 & A_2 \end{pmatrix}$, where

$$A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \cdot \quad \cdot \quad \cdot & \\ a_{kn} & \cdots & a_{kn} \end{pmatrix}, \quad 0 = \begin{pmatrix} 0 & \cdots & 0 \\ & \cdot \quad \cdot \quad \cdot & \\ 0 & \cdots & 0 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} a_{k+1\,n+1} & \cdots & a_{k+1\,m} \\ & \cdot \quad \cdot \quad \cdot & \\ a_{r\,n+1} & \cdots & a_{rm} \end{pmatrix}, \qquad A_3 = \begin{pmatrix} a_{1\,n+1} & \cdots & a_{1m} \\ & \cdot \quad \cdot \quad \cdot & \\ a_{k\,n+1} & \cdots & a_{km} \end{pmatrix}.$$

Definition 12.1. Let α be a linear transformation of $V_h(F)$. Then a subspace M of $V_h(F)$ is an *invariant subspace* of $\alpha \Leftrightarrow \forall\, x \in M$, $x\alpha \in M$.

For any linear transformation there are always at least two invariant subspaces, namely $V_h(F)$ and the subspace consisting of 0 alone. Also, the nullspace of α is an invariant subspace of α. First we have two theorems about invariant subspaces, and then we consider how to determine them.

Theorem 12.1. Let M be an invariant subspace of α, a linear transformation of $V_h(F)$. Let the dimension of M be $r < h$. Then there exists a basis $\{e_i\}$ of $V_h(F)$ such that the matrix of α relative to this basis is $\begin{pmatrix} A_1 & 0 \\ A_3 & A_2 \end{pmatrix}$ where A_1 is an $r \times r$ matrix, 0 is an $r \times (h-r)$ zero matrix, A_2 is an $(h-r) \times (h-r)$ matrix, and A_3 is an $(h-r) \times r$ matrix.

Proof: Let $e_1, \ldots, e_r$ be a basis of M and $e_1, \ldots, e_r, e_{r+1}, \ldots, e_h$ a basis of $V_h(F)$. Then $e_i\alpha = \Sigma_{j=1}^{r} a_{ij}e_i$ for $i = 1, 2, \ldots, r$; $e_i\alpha = \Sigma_{j=1}^{h} a_{ij}e_j$, $i = r+1, \ldots, h$. The form of (a_{ij}) is then as stated. ■

In general, $A_3 \neq 0$. In fact, even if $V_h(F) = M \oplus N$, A_3 is not necessarily zero.

Problem 12.1. Apply Theorem 12.1 to the transformation of $V_3(Q)$ given by: $f_1\alpha = 2f_1 + 5f_3$, $f_2\alpha = f_1 + 2f_2 - 7f_3$, $f_3\alpha = f_1 - 6f_3$, f_1, f_2, f_3 are a basis of $V_3(Q)$. Note that even though $V_3(Q)$ can be expressed as the direct sum of two subspaces, the submatrix $A_3 \neq 0$.

Theorem 12.2. Let M and N be invariant subspaces of α, a linear transformation of $V_h(F)$. Further, let $V_h(F) = M \oplus N$ and dim $M = r$. Then there exists a basis $\{e_i\}$ of $V_h(F) \ni$ the matrix of α relative to the $\{e_i\}$ is $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$, where A_1 is an $r \times r$ matrix and A_2 an $(h-r) \times (h-r)$ matrix.

Proof: Let $e_1, \ldots, e_r$ be a basis of M and $e_{r+1}, \ldots, e_h$ be a basis of N. Then $e_i\alpha = \sum_{j=1}^{r} a_{ij}e_j$, $i = 1, \ldots, r$ and $e_i\alpha = \sum_{j=r+1}^{h} a_{ij}e_j$, $i = r+1, \ldots, h$. So (a_{ij}) has the form specified. ∎

DEFINITION 12.2. Let the vector space E over the field F be the direct sum of the two subspaces M and N which are invariant subspaces of the linear transformation α of E. Let α_1 and α_2 be the restrictions of α to M and N respectively. Then and only then is α called the *direct sum* of α_1 and α_2 and written $\alpha_1 \dotplus \alpha_2 = \alpha$. The subspaces M and N are said to *reduce α completely*. Also the matrix of α is said to be the direct sum of the matrices of α_1 and α_2 and we write $A = A_1 \oplus A_2$, where A_1 and A_2 are the matrices of α_1 and α_2 respectively.

PROBLEM 12.2. Generalize Theorem 12.2 and Definition 12.2 to the case of n subspaces.

In Definition 2.1 of Chapter 5 we defined $f(\alpha)$ where $f(x)$ is a polynomial and α is an element of a ring containing the coefficients of $f(x)$. Now the ring of all linear transformations of a vector space E over a field F contains a subring isomorphic to F (see Problem 12.3 below) and so we may consider polynomials $\in F[x]$, $f(x)$, and consider $f(\alpha)$ where α is a linear transformation of E. We shall let $\mathscr{N}(\alpha)$ and $\mathscr{N}(f(\alpha))$, the latter briefly $\mathscr{N}(f)$, denote the null spaces of the linear transformations α and $f(\alpha)$, respectively.

PROBLEM 12.3. Prove that the ring of all linear transformations of a vector space E over a field F has a subring isomorphic to F. (Hint: Let ι be the identity transformation and then use the mapping $f \leftrightarrow f\iota$ of F into the ring.)

THEOREM 12.3. α is a linear transformation of the vector space E over F, $f(x) \in F[x] \Rightarrow \mathscr{N}(f)$ is an invariant subspace of α.

PROOF. Let $x \in \mathscr{N}(f)$, i.e., $xf(\alpha) = 0$. Now since F is a field, $\alpha f(\alpha) = f(\alpha) \cdot \alpha$. Thus we have $(x\alpha)f(\alpha) = x(\alpha \cdot f(\alpha)) = x(f(\alpha) \cdot \alpha) = (xf(\alpha))\alpha = 0\alpha = 0$. Therefore $x\alpha \in \mathscr{N}(f)$. ∎

THEOREM 12.4. α is a linear transformation of the vector space E over F, $f(x)$, $g(x) \in F[x]$, $g(x) | f(x) \Rightarrow \mathscr{N}(g) \subset \mathscr{N}(f)$.

PROOF. By hypothesis $\exists\, h(x) \in F[x] \ni f(x) = g(x)h(x)$. Then if $x \in \mathscr{N}(g)$, $xg(\alpha) = 0$ and so $xf(\alpha) = x(g(\alpha)h(\alpha)) = (xg(\alpha))h(\alpha) = 0h(\alpha) = 0$. Therefore $x \in \mathscr{N}(f)$. ∎

THEOREM 12.5. α is a linear transformation of the vector space

E over F, $f_i \in F[x]$, $i = 1, 2, \ldots . k$, $d(x) = \underset{\text{(this the g.c.d.)}}{(f_1, f_2, \ldots, f_k)} \Rightarrow$ $\mathcal{N}(d) = \cap_{i=1}^{k} \mathcal{N}(f_i)$.

Proof: By Theorem 12.4, $\mathcal{N}(d) \subset \mathcal{N}(f_i)$, so $\mathcal{N}(d) \subset \cap_{i=1}^{k} \mathcal{N}(f_i)$. By Problem 4.4 of Chapter 5 generalized, $\exists\, s_i(x) \in F[x] \ni d(x) = \Sigma_{i=1}^{k} s_i(x) f_i(x)$. Now if $x \in \cap_{i=1}^{k} \mathcal{N}(f_i)$, then $x(f_i(\alpha)) = 0$, $i = 1, 2, \ldots, k$. So $xd(\alpha) = x\Sigma_{i=1}^{k} s_i(\alpha) f_i(\alpha) = 0$. Therefore, $\cap_{i=1}^{k} \mathcal{N}(f_i) \subset \mathcal{N}(d)$. ■

Theorem 12.6. α is a linear transformation of the vector space E over F, $f_i(x) \in F[x]$, $i = 1, 2, \ldots, k$,

$$h(x) = \underset{\text{(l.c.m)}}{[f_1, f_2, \ldots, f_k]} \Rightarrow \mathcal{N}(h) = \sum_{i=1}^{k} \mathcal{N}(f_i)\,.$$

Proof: Since $f_i | h$, $\mathcal{N}(h) \supset \mathcal{N}(f_i)$, $i = 1, 2, \ldots, k$. Hence, if $x \in \Sigma_{i=1}^{k} \mathcal{N}(f_i)$, $x = \Sigma_{i=1}^{k} x_i$, where $x_i \in \mathcal{N}(f_i)$ and so $x \in \mathcal{N}(h)$. To show that $\mathcal{N}(h) \subset \Sigma_{i=1}^{k} \mathcal{N}(f_i)$, we must show that if $x \in \mathcal{N}(h)$, then we can represent x as $x = \Sigma_{i=1}^{k} x_i$, where $x_i \in \mathcal{N}(f_i)$, $i = 1, 2, \ldots, k$. Since $f_i | h$, $\exists\, q_i, \in F[x] \ni h = q_i f_i$ for each i. Then, using Problem 4.4 of Chapter 5 again, $\exists\, s_i \in F[x] \ni 1 = \Sigma_{i=1}^{k} s_i(x) q_i(x)$, since $(q_1, q_2, \ldots, q_k) = 1$. Then $\Sigma_{i=1}^{k} s_i(\alpha) q_i(\alpha) = \iota$, the identity transformation, and so $x = x\iota = \Sigma_{i=1}^{k} x(s_i(\alpha) q_i(\alpha))$. We shall now show that $x(s_i(\alpha) q_i(\alpha)) \in \mathcal{N}(f_i)$, $\forall\, i$, and this will establish the desired result. Consider $[x(s_i(\alpha) q_i(\alpha))] f_i(\alpha) = x[s_i(\alpha) q_i(\alpha) f_i(\alpha)] = x[s_i(\alpha) h(\alpha)] = x[h(\alpha) s_i(\alpha)] = (xh(\alpha)) s_i(\alpha) = 0 \cdot s_i(\alpha) = 0$. Therefore, x $\in \Sigma_{i=1}^{k} \mathcal{N}(f_i)$. Therefore, $\mathcal{N}(h) = \Sigma_{i=1}^{k} \mathcal{N}(f_i)$. ■

Theorem 12.7. α is a linear transformation of the vector space E over F, $f = f_1 f_2 \cdots f_k, f_1, f_2, \ldots, f_k \in F[x]$, $(f_i, f_j) = 1$ for $i \neq j \Rightarrow$ $\mathcal{N}(f) = \mathcal{N}(f_1) \oplus \mathcal{N}(f_2) \oplus \cdots \oplus \mathcal{N}(f_k)$.

Proof: Since the above conditions imply that $f = [f_1, f_2, \ldots, f_k]$, we have by Theorem 12.6, $\mathcal{N}(f) = \Sigma_{i=1}^{k} \mathcal{N}(f_i)$. Thus to establish the statement of the theorem, we need merely show that this sum is direct. For this it suffices to show that $\mathcal{N}(f_i) \cap \mathcal{N}(f_j) = \{0\}$, for $i \neq j$. Now $(f_i, \Sigma_{j=1, j\neq i}^{k} f_j) = 1$, and so if we apply Theorem 12.5, we have, since $d(x)$ in that theorem is 1, and $\mathcal{N}(\iota) = 0$. $\{0\} = \mathcal{N}(\Pi_{j=1, j\neq i}^{k} f_j) \cap \mathcal{N}(f_i)$, or applying Theorem 12.6 again, we have $\Sigma_{j=1, j\neq i}^{k} \mathcal{N}(f_j) \cap \mathcal{N}(f_i) = \{0\}$ which implies $\mathcal{N}(f_i) \cap \mathcal{N}(f_j) = \{0\}$, for $i \neq j$. ■

Theorem 12.8. α is a linear transformation of $V_n(F) \Rightarrow$ there exists a unique monic polynomial $m(x) \in F[x] \ni m(\alpha) = 0$, and if $g(x) \in F[x]$, $g(\alpha) = 0 \Leftrightarrow m(x)|g(x)$

PROOF For any $a \in V_h(F)$, the set $a, a\alpha, a\alpha^2, \dots, a\alpha^t$ must be linearly dependent for some $t \leqslant h$, since any $h+1$ elements of $V_h(F)$ are linearly dependent Let t be chosen as small as possible, and then for $c_i \in F$ we have $\Sigma_{i=1}^{t} c_i a\alpha^i = 0$ Let $g(x) = \Sigma_{i=1}^{t} c_i x^i$ and then $ag(\alpha) = 0$ Let $e_1, e_2, \dots, e_h$ be a basis for $V_h(F)$ and let $g_i(x)$ be chosen for each e_i, $i = 1, 2, \dots, h$ as was done above for a Let $f(x) = [g_1, g_2, \dots, g_h]$ Then by Theorem 12 4, $e_i f(\alpha) = 0$ for each i Now let $y \in V_h(F)$ then $y = \Sigma_{i=1}^{h} y_i e_i$ and since $f(\alpha)$ is linear (cf Problem 12 4 below) $yf(\alpha) = 0$ Therefore, $f(\alpha) = 0$ It is evident that the set of all elements $h(x) \in F[x] \ni h(\alpha) = 0$ form an ideal in $F[x]$ By Corollary 8 1 of Chapter 5 this ideal is a principal ideal Let the monic generator of this ideal be $m(x)$ Then $m(x)$ has the properties stated in the theorem ∎

PROBLEM 12 4 Prove that if $f(x) \in F[x]$ if α is a linear transformation of the vector space E over F then $f(\alpha)$ is a linear transformation of E

PROBLEM 12 5 Find the polynomial $m(x)$ of the last theorem for the linear transformation of Problem 12 1 (Hint use the method of the proof of the theorem)

DEFINITION 12 3 The polynomial $m(x)$ whose existence is established by Theorem 12 8 is called the *minimum polynomial of the linear transformation* α

13 MINIMUM POLYNOMIALS

In this section we shall consider minimum polynomials of linear transformations and of elements of a vector space relative to a linear transformation

THEOREM 13 1 Let $m(x)$ be the minimum polynomial of the linear transformation α of $V_h(F)$ and let $m(x) = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ be the factorization of $m(x)$ into a product of powers of distinct monic polynomials each irreducible in $F[x]$ Let $L_i = \mathcal{N}(p_i^{h_i})$, $i = 1, 2, \dots, s$ Then $L_1, L_2, \dots, L_s$ reduce α completely i e $V_h(F) = L_1 \oplus L_2 \oplus \cdots \oplus L_s$ and $\alpha = \alpha_1 + \alpha_2 + \cdots + \alpha_s$ where α_i is the linear transformation of L_i which is the restriction of α to L_i The matrix of α is the direct sum of the matrices of the α_i, and each matrix of the α_i is a $t_i \times t_i$ matrix where t_i is the dimension of $\mathcal{N}(p_i^{h_i})$ Lastly the minimum polynomial of α_i is $p_i^{h_i}$

PROBLEM 13.1. Prove Theorem 13.1. [Hint: most of the theorem follows from the preceding theorems once it is realized that $\mathcal{N}(m(\alpha)) = V_h(F)$.]

In the next four exercises the reader is asked to find the minimum polynomial for a given matrix (i.e., for the transformation which has the given matrix as matrix). Either the method used in the proof of Theorem 12.8 may be employed or the following: let

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Since this is obviously not a multiple of I, we compute

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

and see if there exist $a_2, a_1, a_0 \in Q \ni a_2A^2 + a_1A + a_0I = 0$; i.e.,

$$a_2\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + a_1\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + a_0\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

By looking at the element of $a_2A^2 + a_1A + a_0I$ in position (1,1), we see that $a_0 = 0$; in position (1,2) that $a_1 = 0$; and finally in position (1,3) that $a_2 = 0$. Thus A^2, A, I are not linearly dependent and so the degree of the minimum polynomial is at least 3 and so we try using I, A, A^2, A^3. We shall prove later that the degree of the minimum polynomial of an $h \times h$ matrix is $\leqslant h$.

PROBLEM 13.2. Find the minimum polynomial of the above A.

PROBLEM 13.3. Do the same for $B = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$

PROBLEM 13.4. Do the same for $C = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$

PROBLEM 13.5. Show that $D = \begin{pmatrix} 0 & -1 & 2 \\ -1 & 1 & 1 \\ -1 & -1 & 3 \end{pmatrix}$ has the same minimum polynomial as C.

PROBLEM 13.6. Factor the minimum polynomial $m(x)$ of the matrix C into a product of powers of polynomials, irreducible in

$Q[x]$ as in Theorem 13 1 It will turn out that $m(x) = p_1^2 p_2$ Find $\mathcal{N}(p_1^2)$ and $\mathcal{N}(p_2)$ and prove that $V_3(Q)$ is their direct sum Then express C in the form of Theorem 12 2 Verify that p_1^2 and p_2 are the minimum polynomials for the matrices C_1 and C_2 respectively in that representation of C

PROBLEM 13 7 Do the same as in Problem 13 6 for A and B

PROBLEM 13 8 Keeping in mind Definition 11 2 Theorems 11 5 12 2 and the results of the exercises above find for the matrix A and the representation $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ of Problem 13 7 the matrix of Definition 11 2

PROBLEM 13 9 Do the same as in Problem 13 8 for C D and B

THEOREM 13 2 α is a linear transformation of $V_h(F)$ $a \in V_h(F) \Rightarrow \exists n \in Z$ and $c_i \in F$ not all c_i zero $i = 0$ 1 $n \ni \sum_{i=0}^{n} c_i(a\alpha^i) = 0$

PROOF If $a \in V_h(F)$ then the set a $a\alpha$ $a\alpha^2$ $a\alpha^h$ must be linearly dependent since they are $h + 1$ elements of $V_h(F)$ Thus there must exist a relation of the form of the theorem where $n \leq h$ ■

COROLLARY 13 1 Under the conditions of Theorem 13 2 there exists a unique monic polynomial $m_a(x) \in F[x]$ of minimum degree $\ni a m_a(\alpha) = 0$ and $\ni a g(\alpha) = 0$ for $g(x) \in F[x] \Rightarrow m_a(x) | g(x)$

PROOF By Theorem 13 2 there exists at least one $f(x) \in F[x] \ni af(\alpha) = 0$ Let $g(x) \in F[x]$ be another such polynomial Then $a[f(\alpha) + g(\alpha)] = af(\alpha) + ag(\alpha) = 0$ and $\forall h(x) \in F[x]$ $a[f(\alpha)h(\alpha)] = \{af(\alpha)\}h(\alpha) = 0h(\alpha) = 0$ $a[h(\alpha)f(\alpha)] = a[f(\alpha) h(\alpha)] = [af(\alpha)]h(\alpha) = 0$ Therefore the set of all $f(x) \in F[x] \ni af(\alpha) = 0$ is an ideal All ideals in $F[x]$ are principal Therefore $\exists$ monic $m_a(x) \in F[x]$ which generates this ideal and that it is unique and $ag(\alpha) = 0 \Rightarrow m_a(x) | g(x)$ follow from the well known properties of principal ideals ■

DEFINITION 13 1 The unique monic polynomial $m_a(x)$ whose existence is established in Corollary 13 1 is called the *order of a relative to α*

PROBLEM 13 10 Prove that the degree of the order of a is less than or equal to degree of the minimum polynomial of α

PROBLEM 13.11. Find the orders of (1,2,0) and (0,0,1) for the linear transformation whose matrix is C of Problem 13.4. (Hint: in this and several of the following exercises, the reader might find it convenient in finding $a\alpha$, to regard it as

$$(a_1, a_2, \ldots, a_h)\begin{pmatrix} a_{11} & \cdots & a_{1h} \\ & \cdots & \\ a_{h1} & \cdots & a_{hh} \end{pmatrix}.$$

PROBLEM 13.12. Find the orders of (1,3,−1) and (0,−1,1) for the linear transformation whose matrix is D of Problem 13.5.

PROBLEM 13.13. Do the same as in Problem 13.11 for B of Problem 13.3.

PROBLEM 13.14. Show that in the above three exercises, the orders divide the minimum polynomials of the linear transformations.

PROBLEM 13.15. Find the orders of the sum of the two vectors in Problems 13.11, 13.12, 13.13.

PROBLEM 13.16. Find the order of (1,2,0) for D of Problem 13.5.

14. CYCLIC SPACES AND TRANSFORMATIONS

DEFINITION 14.1. The subspace generated by $a, a\alpha, a\alpha^2, \ldots,$ where $a \in V_h(F)$ and α is a linear transformation of $V_h(F)$, is the *cyclic space generated by a under α*, and is denoted by $\{a\}$.

THEOREM 14.1. The cyclic space generated by $a \in V_h(F)$ is an invariant subspace of α.

PROOF: Let $v \in \{a\}$. Then $v = c_0a + c_1a\alpha + c_2a\alpha^2 + \cdots + c_na\alpha^n = af(\alpha)$, where $f(x) = \Sigma_{i=0}^{n}\ c_ix^i$. Then $v\alpha = af(\alpha)\alpha \in \{a\}$. ∎

COROLLARY 14.1. $\{a\}$ is the smallest invariant subspace of α which contains a.

PROBLEM 14.1. Find $\{a\}$ for the vectors given in Problems 13.11, 13.12, 13.16.

COROLLARY 14.2. $m_a(x)$ is the minimum polynomial for the linear transformation of $\{a\}$, which is the restriction in $\{a\}$ of α.

COROLLARY 14.3. $m(x)$ for α is a multiple of $m_a(x)$ $\forall\, a \in V_h(F)$.

Problem 14.2 Prove Corollaries 14.2 and 14.3.

Problem 14.3 Show by an example that even though $V_n(F) = L_1 \oplus L_2$ where $L_i = \{a_i\}$, $i = 1, 2$, the minimum polynomial of α need not be the product of $m_{a_1}(x)$ and $m_{a_2}(x)$.

Theorem 14.2 If the orders $m_i(x)$ of $f_i \in V_n(F)$, $i = 1, 2, \ldots, r$, are relatively prime in pairs, then the order of $f = f_1 + f_2 + \cdots + f_r$ is the product $m_1(x)m_2(x)\cdots m_r(x) = n(x)$.

Proof $f_i m_i(\alpha) = 0$, $i = 1, 2, \ldots, r$, and so $f_i n(\alpha) = 0$, $i = 1, 2, \ldots, r$. Therefore $f n(\alpha) = \Sigma_{i=1}^r f_i n(\alpha) = 0$ and so $m_f(x) | n(x)$. Now let $s_1(x) = m_f(x) m_2(x) m_3(x) \cdots m_r(x)$. Then $f s_1(\alpha) = 0$ and $f_j s_1(\alpha) = 0$ for $j = 2, 3, \ldots, r$. Therefore, since $f s_1(\alpha) = f_1 s_1(\alpha) + f_2 s_1(\alpha) + \cdots + f_r s_1(\alpha)$, we have $f_1 s_1(\alpha) = 0$. Therefore $m_1(x) | s_1(x)$ and since $(m_1(x), m_i(x)) = 1$ for $i = 2, 3, \ldots, r$, $m_1(x) | m_f(x)$. Similarly $m_i(x) | m_f(x)$, $i = 1, 2, \ldots, r$. Therefore $n(x) | m_f(x)$ and so, since both $n(x)$ and $m_f(x)$ are monic, we have $n(x) = m_f(x)$. ∎

Definition 14.2 Let α be a linear transformation of $V_n(F)$. Then a set of elements $e_1, e_2, \ldots, e_n \in V_n(F)$ *generate $V_n(F)$ relative to α* $\Leftrightarrow \forall\, u \in V_n(F)\ \exists\, \phi_i(x) \in F[x] \ni u = \Sigma_{i=1}^n e_i \phi_i(\alpha)$.

Such a set of elements always exists since $V_n(F)$ has an ordinary basis and this generates $V_n(F)$ in the above sense with all the $\phi_i(x) \in F$.

Theorem 14.3 $m(x)$ is the minimum polynomial of α, a linear transformation of $V_n(F) \Rightarrow \exists\, f \in V_n(F) \ni m_f(x) = m(x)$.

Proof Let $e_1, e_2, \ldots, e_n$ generate $V_n(F)$ relative to α and let $m(x) = [m_{e_1}(x), m_{e_2}(x), \ldots, m_{e_n}(x)]$. Now $m_{e_i}(x) | m(x)$ and so $m(x) | m(x)$.

On the other hand, if $u = \Sigma_{i=1}^n e_i \phi_i(\alpha)$, then $u m(\alpha) = \Sigma_{i=1}^n e_i \phi_i(\alpha) m(\alpha) = \Sigma\, e_i m(\alpha) \phi_i(\alpha) = 0 \Rightarrow m(\alpha) = 0 \Rightarrow m(x) | m(x)$ by Theorem 12.8. Hence $m(x) = m(x)$.

Now let $m_{e_i}(x) = (p_1(x))^{k_{i1}} (p_2(x))^{k_{i2}} \cdots (p_r(x))^{k_{ir}}$ where $p_j(x)$ is monic and irreducible in $F[x]$, $i = 1, 2, \ldots, n$, and $p_i(x) \neq p_j(x)$ if $i \neq j$. Then if $k_j = \max(k_{1j}, k_{2j}, \ldots, k_{nj})$, $j = 1, 2, \ldots, r$, we have $m(x) = (p_1(x))^{k_1} (p_2(x))^{k_2} \cdots (p_r(x))^{k_r}$.

If the order of u, $m_u(x) = t_1(x)t_2(x)$, then $v = u t_1(\alpha)$ has order $t_2(x)$, since $v t_2(\alpha) = 0$, and if $v d(\alpha) = 0$ where $d(x) \in F[x]$, then $u t_1(\alpha) d(\alpha) = 0 \Rightarrow t_1(x) t_2(x) | t_1(x) d(x) \Rightarrow t_2(x) | d(x)$ and so $t_2(x)$ is the order of v.

Thus if $k_1 = k_{1n}$, the order of $f_1 = e_1(p_2(\alpha))^{k_{2n}}(p_3(\alpha))^{k_{3n}} \cdots (p_r(\alpha))^{k_{rn}}$ is $(p_1(x))^{l_1}$. Similarly, we can find f_j. $j = 2, 3, \ldots, r \ni f_j$ has order $(p_j(x))^{l_j}$. Then, by Theorem 14.2, $f = f_1 + f_2 + \cdots + f_r$ has order $m(x)$. ■

Problem 14.4. Find vectors f of the type of Theorem 14.3 for each of the linear transformations of Problems 13.2, 13.3, 13.4, 13.5.

Definition 14.3. The linear transformation α of $V_h(F)$ is called *cyclic* (also called *nonderogatory*) $\Leftrightarrow \exists\ e \in V_h(F) \ni$ the cyclic space generated by e under α is $V_h(F)$.

Corollary 14.4. The minimum polynomial of a linear transformation of $V_h(F)$ has degree $\leqslant h$.

Problem 14.5. Prove Corollary 14.4.

Problem 14.6. Determine which linear transformations studied so far are cyclic.

Theorem 14.4. A linear transformation α of $V_h(F)$ is cyclic $\Leftrightarrow$ the degree of the minimum polynomial is h.

Proof: The implication $\Rightarrow$. If α is cyclic, $\exists\ e \ni \{e\} = V_h(F)$ is cyclic $\Rightarrow$ deg $m_e(x) = h$, and so by Corollary 14.3, deg $m(x) \geqslant h$, but by Corollary 14.4, deg $m(x) \leqslant h$. Therefore, deg $m(x) = h$ and $m_e(x) = m(x)$.

The implication $\Leftarrow$. If deg $m(x) = h$, then by Theorem 14.3, $\exists\ e \ni m_e(x) = m(x)$. Then deg $m_e(x) = h$, and so dim $\{e\} = h$. Therefore, by Problem 6.4 of Chapter 4, $\{e\} = V_h(F) \Rightarrow \alpha$ is cyclic. ■

Theorem 14.5. If α is a cyclic linear transformation of $V_h(F)$, there exists a basis of $V_h(F)$ such that relative to this basis the matrix of α is

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & a_3 & \cdots & a_{h-1} \end{pmatrix}$$

where $m(x) = x^h - a_{h-1}x^{h-1} - \cdots - a_1x - a_0$ is the minimum polynomial of α.

Proof: By Theorem 14.3, $\exists\ e \in V_h(F) \ni \{e\} = V_h(F)$. Then

e $e\alpha$ $e\alpha^2$ $e\alpha^{h-1}$ is a basis of $V_h(F)$ and if we let $e_i = e\alpha^{i-1}$ we have

$$
\begin{aligned}
e_1\alpha &= e_2\\
e_2\alpha &= e_3\\
\\
e_{h-1}\alpha &= e_h\\
e_h\alpha &= a_0e_1 + a_1e_2 + a_2e_3 + \quad + a_{h-1}e_h
\end{aligned}
$$ ■

DEFINITION 14 4 The matrix in Theorem 14 5 is called the *companion matrix of* $m(x)$ This matrix is called the *Jordan canonical matrix* of the linear transformation α

THEOREM 14 6 If C is the companion matrix of $m(x)$ then the Smith normal form (cf Theorem 10 1) of $xI - C$ is diag (1 1 1 $m(x)$)

PROBLEM 14 7 Prove Theorem 14 6

PROBLEM 14 8 Use any of the linear transformations found in Problem 14 6 to be cyclic and verify Theorem 14 5 for the chosen case

The form of the matrix in Theorem 14 5 displays the minimum polynomial of the cyclic transformation but not its factorization We shall now develop a matrix of α which displays the factorization of $m(x)$ into factors irreducible in $F[x]$ Thus the first form is unchanged when we go to an extension field of F while the second will in general change

We shall first consider the special case in which $m(x) = (p(x))^k$ where $p(x)$ is irreducible in $F[x]$ For ease in reference we are going to prove the theorem first and then state it Let $p(x) = x^q - a_{q-1}x^{q-1} - \quad - a_1x - a_0$ Then of course $\deg m(x) = h - kq$ Further let $e \in V_h(F)$ and be such that $\{e\} = V_h(F)$ We shall now define some vectors which form a basis of $V_h(F)$

$$
\begin{array}{lll}
f_1 = e(p(\alpha))^{k-1} & f_2 = e(p(\alpha))^{k-1}\alpha & f_q = e(p(\alpha))^{k-1}\alpha^{q-1}\\
f_{q+1} = e(p(\alpha))^{k-2} & f_{q+2} = e(p(\alpha))^{k-2}\alpha & f_{2q} = e(p(\alpha))^{k-2}\alpha^{q-1}\\
\\
f_{(k-1)q+1} = e & f_{(k-1)q+2} = e\alpha & f_{kq} = e\alpha^{q-1}
\end{array}
$$

Each f is of the form $e\phi(\alpha)$ where $\deg \phi(x) < kq - h$ Furthermore no two of the ϕ s have the same degree Then the kq f s are linearly independent over F since a linear relation between them would give rise to a polynomial $s(x) \in F[x] \ni es(\alpha) - 0$ contrary to our hypothesis that α is cyclic. Therefore, the f's form a basis of $V_h(F)$.

The matrix of α relative to $f_1, f_2, \ldots, f_{kq}$ is obtained in the usual way as follows:

$$\begin{aligned}
f_1\ \alpha &= f_2 \\
f_2\ \alpha &= \qquad f_3 \\
&\ \vdots \\
f_{q-1}\alpha &= \qquad\qquad f_q \\
f_q\ \alpha &= e(p(\alpha))^{k-1\ q} = e(p(\alpha))^{k-1}[\alpha^q = p(\alpha)] \\
&= e(p(\alpha))^{k-1}[a_0\iota + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}] \\
&= a_0f_1 + a_1f_2 + a_2f_3 + \cdots + a_{q-1}f_q \\
f_{q+1}\ \alpha &= \qquad f_{q+2} \\
f_{q+2}\ \alpha &= \qquad\qquad f_{q+3} \qquad\qquad (1) \\
&\ \vdots \\
f_{2q-1}\alpha &= \qquad\qquad f_{2q} \\
f_{2q}\quad &= e(p(\alpha))^{k-2\ q} = e(p(\alpha))^{k-2}\,[\alpha^q - p(\alpha)] + e(p(\alpha))^{k-1} \\
&= a_0f_{q+1} + a_1f_{q+2} + a_2f_{q+3} + \cdots + a_{q-1}f_{2q} + f_1 \\
&\ \vdots \\
f_{(k-1)q+1}\alpha &= \qquad f_{(k-1)q+2} \\
f_{(k-1)q+2}\alpha &= \qquad\qquad f_{(k-1)q+3} \\
&\ \vdots \\
f_{kq}\ \alpha &= \qquad a_0f_{(k-1)q+1} + a_1f_{(k-1)q+2} + \cdots + a_{q-1}f_{kq} + f_{(k-1)+1}\,.
\end{aligned}$$

Hence, the matrix of α, relative to the basis $f_1, f_2, \ldots, f_k$, has the form (2)

$$\begin{pmatrix}
C & & & 0 \\
D & C & & \\
 & D & \ddots & \\
0 & & \ddots & \\
 & & D & C
\end{pmatrix} \tag{2}$$

where C is the companion matrix of $p(x)$ and D is the $q \times q$ matrix (3):

$$D = \begin{pmatrix}
0 & 0 & & 0 \\
0 & 0 & \cdots & 0 \\
 & \cdot & \cdot & \cdot \\
1 & 0 & \cdots & 0
\end{pmatrix}. \tag{3}$$

THEOREM 14.7. If α is a cyclic linear transformation of $V_h(F)$ with minimum polynomial $m(x) = (p(x))^k$, where $p(x) = x^q - a_{q-1}x^{q-1} - \cdots - a_1x - a_0$ is irreducible in $F[x]$, then there exists a basis of $V_h(F)$ such that relative to this basis the matrix of α has the form

(2) where C is the companion matrix of $p(x)$, and D is given by (3).

If the reader is in doubt about some of the details of the preceding he might find it clarifying to write out a few more steps in equations (1).

THEOREM 14.8 If α is a cyclic linear transformation of $V_n(F)$ with minimum polynomial $m(x) = m_1(x)m_2(x)\cdots m_r(x)$, where the $m_i(x)$ are relatively prime in pairs, then $\exists\, e_1, e_2, \ldots, e_r \in V_n(F) \ni V_n(F) = \{e_1\} \oplus \{e_2\} \oplus \cdots \oplus \{e_r\}$ and $m_{e_i}(x) = m_i(x)$.

PROOF Let $n_i(x) = m(x)/m_i(x)$ and let $e_i = e n_i(\alpha)$ where e is a generator of $V_n(F)$ relative to α. Then since α is cyclic $m_{e_i}(x) = m_i(x)$. By Theorem 14.2 the order of $e = e_1 + e_2 + \cdots + e_r$ is $m(x)$. Hence $\{e\} = V_n(F)$ and so $V_n(F) = \{e_1\} + \{e_2\} + \cdots + \{e_r\}$. Because of the dimensions this sum must be direct. ■

THEOREM 14.9 If α is a cyclic linear transformation of $V_n(F)$ with minimum polynomial $m(x) = (p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_r(x))^{k_r}$ where the $p_i(x)$ are monic irreducible in $F[x]$ and relatively prime in pairs, then there exists a basis of $V_n(F)$ such that relative to this basis the matrix of α has the form (4) where each H_i is of the form

$$\begin{pmatrix} H_1 & & \\ & H_2 & \\ & & H_r \end{pmatrix} \tag{4}$$

(2) and is determined from $(p_i(x))^{k_i}$ in the same way as the matrix (2) was determined from $(p(x))^k$.

PROOF Apply Theorem 14.7 and then Theorem 12.2. ■

Now we state and prove a proposition which is useful in the proof of a later theorem and also is useful in applying the last few theorems.

THEOREM 14.10 Let $(n(x))^k$ be the highest power of $n(x)$ which divides the minimum polynomial $m(x)$ of the linear transformation α of $V_n(F)$, where $n(x)$ is irreducible in $F[x]$, and let $S_i = \mathscr{N}((n(\alpha))^i)$, $i = 0, 1, \ldots, k$. Then $\exists\, a \in S_i \ni a \notin S_{i-1}$ for $i \leq k$.

PROOF $(n(x))^{i+1} = n(x)(n(x))^i$ and so by Theorem 12.4 $S_i \subset S_{i+1}$. We must show that the inclusion relation is a strict inclusion. Suppose that $S_i = S_{i+1}$ for some $i \leqq k-1$; then the nullity of $(n(\alpha))^i$ = nullity of $(n(\alpha))^{i+1}$ and so by Theorem 3.3 rank of $(n(\alpha))^i$ = rank of $(n(\alpha))^{i+1}$ and so if A is the matrix of α, $(n(A))^i$ is equivalent to $(n(A))^{i+1}$. Therefore there exists nonsingular $P \ni (n(A))^i =$

$P(n(A))^{i+1}$. On multiplying both sides by $(n(A))^{k-i-1}g(A)$, where $g(x) = m(x)/(n(x))^k$, we then have $f(A) = 0$, where $f(x) = (n(x))^{k-1} m(x)/(n(x))^k$ is of degree less than the degree of $m(x)$, which is impossible. Therefore, $\exists\, a \in S_i$ and $a \notin S_{i-1}$. ■

PROBLEM 14.9. For C of Problem 13.4 find $a_1 \in \mathcal{N}(x-1) \ni a_1 \notin \mathcal{N}((x-1)^0)$; $a_2 \in \mathcal{N}((x-1)^2) \ni a_2 \notin \mathcal{N}(x-1)$.

PROBLEM 14.10. Do the same for B of Problem 13.3.

DEFINITION 14.5. The matrix (4) of Theorem 14.9 is called the *classical canonical matrix* of the cyclic linear transformation α.

PROBLEM 14.11. Find classical canonical matrices for A, C, D of Problems 13.1, 4, 5.

15. NONCYCLIC LINEAR TRANSFORMATIONS

We shall now consider a noncyclic linear transformation α of $V_h(F)$. We shall, as we did for Theorem 14.7, prove the theorem first and then state it. Let $m(x)$ be the minimum polynomial of α and we shall first consider the case in which $m(x) = (p(x))^k$, where $p(x) = x^q - a_{q-1}x^{q-1} - \cdots - a_1x - a_0$ is irreducible in $F[x]$. By Theorem 14.3, $\exists\, e_1 \ni m_{e_1}(x) = m(x)$ and let $M_1 = \{e_1\}$. If α is not cyclic, then $\exists\, a \in V_h(F) \ni a \notin M_1$. For every $u \in V_h(F)$, $u(p(\alpha))^k = 0$, $u(p(\alpha))^0 = u$, and so $\exists\, k_u \in Z^* \ni u(p(\alpha))^{k_u} \in M_1$ while $u(p(\alpha))^{k_u-1} \notin M_1$. Now of the set of all $a \in M_1$, choose one, call it u, such that the k_u just discussed is maximum. Now, finally, rename it e_2' and call $k_{e_2'}$, k_2. Then $e_2'(p(\alpha))^{k_2} = e_1g(\alpha)$, where $g(x) \in F[x]$ and is of degree $< kq$. Now $\exists\, q(x), r(x) \in F[x] \ni g(x) = (p(x))^{k_2} q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < k_2q$. Then $e_2'(p(\alpha))^{k_2} = e_1q(\alpha)(p(\alpha))^{k_2} + e_1r(\alpha)$. On multiplying by $(p(\alpha))^{k-k_2}$, we have $e_2'm(\alpha) = e_1q(\alpha)m(\alpha) + e_1(P(\alpha))^{k-k_2}r(\alpha)$. Therefore, $e_1(p(\alpha))^{k-k_2} r(\alpha) = 0$. But $(p(x))^{k-k_2}r(x)$ is of degree $< (k - k_2q + k_2q = kq$ and the order of e_1 is of degree kq. Therefore, $r(x) = 0$. Therefore, $e_2'(p(\alpha))^{k_2} = e_1q(\alpha)(p(\alpha))^{k_2}$.

Now we define $e_2 = e_2' - e_1q(\alpha)$. Then $e_2(p(\alpha))^{k_2} = 0 \in M_1$. This element e_2 has the same maximal k_u as e_2', since $e_2(p(\alpha))^{k_2} = e_2'(p(\alpha))^{k_2-1} - e_1(p(\alpha))^{k_2-1}q(\alpha)$; if $e_2(p(\alpha))^{k_2-1} \in M_1$, since $e_1(p(\alpha))^{k_2-1}q(\alpha) \in M_1$, we should have $e_2'(p(\alpha))^{k_2-1} \in M_1$, which is contrary to the choice of e_2'.

Finally, we must prove that there is no polynomial, $s(x) \in F[x]$, of lower degree than $k_2q \ni e_2s(\alpha) = 0$. For that, let $s(x) \in F[x]$

and $es(\alpha) - 0$ Then if $d(x)$ is a g c d of $s(x)$ and $(p(x))^{k_2}$ $\exists\, a(x)$ $b(x) \in F[x] \ni d(x) - s(x)a(x) + (p(x))^{k_2}b(x)$ Hence $e_2d(\alpha) - e_2s(\alpha)a(\alpha) + e_2(p(\alpha))^{k_2}b(\alpha)$ Since the two terms on the right $\in M_1$ $e_2d(\alpha) \in M$ But since $d(x)|(p(x))^{k_2}$ $d(x) - (p(x))^{w}$ where $0 < w \; < k_2$ But since $e_2d(\alpha) \in M_1$ and because of the choice of k_2 $w = k_2$ and so $s(x) = (p(x))^{k_2}t(x)$

Now we define g_1 g g_{k_2q} precisely as f f_2 f_{kq} were defined in the proof of Theorem 14 7 with the e and k of that development replaced by e_2 and k_2 respectively

The g s just defined are linearly independent and the set consisting of the f s and the g s is linearly independent for otherwise we should have a relation $e_2f(\alpha) - e\, g(\alpha)$ where $f(x)$ and $g(x) \in F[x]$ and are of degree $< k\, q$ and kq respectively By the reasoning given above for $s(x)$ we see that $f(x)$ must be divisible by $(p(x))^{k_2}$ which is of degree k_2q Therefore in the supposed relation $f(x)$ must be zero and so linear independence is established

Finally from the form of the g s it is clear that the subspace generated by them is an invariant subspace relative to α and the effect of α is given by a set of equations precisely of the form of the equations (1) in the proof of Theorem 14 7 with the f s replaced by the g s and k replaced by k_2

Let $M_2 - \{e_2\}$ Then if $V_n(F) - M \oplus M_2$ [by the above if $V_n(F)$ is the sum of M and M it is clearly the direct sum] then the matrix of α relative to the f s and g s is $\begin{pmatrix} D & 0 \\ 0 & D_2 \end{pmatrix}$ where D are of the form (2) of Theorem 14 7 [Note the D here are formed for the same polynomial whereas in the case of the matrix in Theorem 14 9 each H is formed for a different polynomial]

If $V_n(F) \neq M \oplus M_2$ then $\exists\, u \in V(F) \ni u \notin M \oplus M_2$ and we proceed as before to get another invariant subspace M_3 with no vectors in common with M and M_2 except 0 We can continue in this manner until we have $V_n(F) - M_1 \oplus M_2 \oplus \quad \oplus M_s$ and we have

THEOREM 15 1 If α is a linear transformation of $V_n(F)$ with minimum polynomial $m(x) - (p(x))^k$ where $p(x)$ is irreducible in $F[x]$ then there exists a basis of $V_n(F)$ such that relative to this basis the matrix of α has the form (5) where each D is of the form (2)

$$(5) \qquad \begin{pmatrix} D & & 0 \\ & D_2 & \\ 0 & & D_s \end{pmatrix}$$

of the matrix in Theorem 14.7 and is the matrix of a cyclic linear transformation of a subspace of $V_h(F)$. Each D_i is formed from some power of $p(x)$.

If $m(x) = (p_1(x))^{k_1}(p_2(x))^{k_2} \cdots (p_r(x))^{k_r}$, where $p_i(x)$ is irreducible in $F[x]$, for $i = 1, 2, \ldots, r$, and the $p_i(x)$ are relatively prime in pairs, then we can apply Theorem 14.9 to express $V_h(F)$ as the direct sum of the null spaces of $(p_i(x))^{k_i}$. By the previous development, each null space is expressible as the direct sum of invariant spaces. Thus, $V_h(F)$ is expressible as a direct sum of invariant subspaces of the type discussed above. Hence,

Theorem 15.2. If α is a linear transformation of $V_h(F)$, then α is expressible as a direct sum of cyclic linear transformations and there exists a basis of $V_h(F)$ such that relative to this basis, the matrix of α is the direct sum of matrices of the type of (2) of Theorem 14.7.

16. INVARIANT FACTORS AND SIMILARITY INVARIANTS

Definition 16.1. The diagonal elements different from 0 in the Smith normal form of a matrix as given in Theorem 10.1 are called the *invariant factors* of A. The invariant factors of $xI - A$ where $A \in F^{s \times s}$ are called the *similarity invariants* of A.

Theorem 16.1. The matrix A is similar to the matrix $B \Leftrightarrow A$ and B have the same similarity invariants.

Proof: Follows immediately from Theorem 10.1 and Theorem 11.6. ∎

Theorem 16.2. A matrix A is similar to the direct sum of the companion matrices of its similarity invariants.

Problem 16.1. Prove Theorem 16.2.

Definition 16.2. The set of all powers of irreducible factors of the similarity invariants of the matrix A, which actually occur in the similarity invariants, are called the *elementary divisors* of the matrix A.

Theorem 16.3. A matrix A is similar to the direct sum of the companion matrices of its elementary divisors.

Problem 16.2. Prove Theorem 16.3.

For Problems 16.3 through 16.7 use

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 2 & 3 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 3 \end{pmatrix}$$

Problem 16 3 Show that the minimum polynomial of A is $x^3 - 3x - 2$ that of B is $x^2 - 3x - 2$

Problem 16 4 Show that the Smith normal form of $xI - A$ is

$$\begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ 0 & & x+1 & \\ & & & m(x) \end{pmatrix} \text{ that of } xI - B \text{ is } \begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ 0 & & m(x) & \\ & & & m(x) \end{pmatrix}.$$

where in each case $m(x)$ is the minimum polynomial of A or B, respectively

Problem 16 5 Find a basis of $V_4(Q)$ of the type developed in the proof of Theorem 15 1 for A and for B

Problem 16 6 Verify that A and B are in the forms given in the preceding theorems with respect to the bases found in Problem 16 5

Problem 16 7 Give a matrix with similarity invariants $(x-1)^2(x^2+1)$ $(x-1)^7(x^2+1)^2(x^3+3x+5)$

Problem 16 8 Do the same as in Problem 16 7 over $F = Q(i)$

Definition 16 3 Let $h_1(x)$ $h_2(x)$ $h_r(x)$ be the similarity invariants of the matrix A Then the polynomial $f(x) = \Pi_{i=1}^r h_i(x)$ is the *characteristic polynomial* of A

Theorem 16 4 The last similarity invariant of a matrix is the minimum polynomial of A

Corollary 16 1 (The Hamilton–Cayley Theorem) If $f(x)$ is the characteristic polynomial of the matrix A then $f(A) = 0$

Problem 16 9 Prove Theorem 16 4

Problem 16 10 Prove Corollary 16 1

Bibliography

General

Albert, A. A., *Fundamental Concepts of Higher Algebra,* 1956, Univ. of Chicago Press, Chicago.

Albert, A. A., *Modern Higher Algebra,* 1937, Univ. of Chicago Press, Chicago.

Birkhoff, G. and MacLane S., *A Survey of Modern Algebra,* 1965, MacMillan, New York.

Bourbaki, N., *Algebre,* Chapitres I–IX, Actualités Sci. Ind. 1144, 1951; 1236, 1955, 1044, 1948; 1102, 1950; 1179, 1952; 1261, 1958; 1272, 1959, Hermann, Paris.

Chevalley, C., *Fundamental Concepts of Algebra,* 1956, Academic Press, New York.

Hasse, H., *Hohere Algebra,* Vol. I, 1933, Vol. II, 1937, de Gruyter, Berlin. English translation, T. J. Benac, *Higher Algebra,* 1954, Ungar, New York.

Hu, S., *Elements of Modern Algebra,* 1965, Holden-Day, San Francisco.

Jacobson N., *Lectures in Abstract Algebra,* Vol. I, 1951, Vol. II, 1953, Vol. III, 1964, van Nostrand, Princeton.

Kurosh, A. G., *General Algebra,* 1963, Chelsea, New York.

MacDuffee, C. C., *Introduction to Abstract Algebra,* 1940, Wiley, New York.

van der Waerden, *Moderne Algebra,* Vol. I, 1937, Vol. II, 1931, Springer, Berlin. English Translation, F. Blum, *Modern Algebra,* 1953, Ungar, New York.

Zariski, O. and Samuel, P., *Commutative Algebra,* Vol. I, 1958, Vol. II, 1960, van Nostrand, Princeton.

Specialized

Burnside, W., *The Theory of groups of Finite Order,* 1911, Cambridge Univ. Press, Cambridge.

Halmos, P. R., *Finite-Dimensional Spaces,* 1958, van Nostrand, Princeton.

Hardy, G. and Wright, E., *An Introduction to the Theory of Numbers,* 1938, Oxford Univ. Press, Oxford.

Hohn, F., *Elementary Matrix Algebra,* 1958, MacMillan, New York.

Kurosh, A. G., *The Theory of Groups,* Vols. I and II, 1960, Chelsea, New York.

MacDuffee C C *Vectors and Matrices* **1943** Mathematical Association of America Buffalo

McCoy N H *Rings and Ideals* **1948** **Mathematical** Association of America Buffalo

Pollard H *The Theory of Algebraic Numbers* 1950 Mathematical Association of America **Buffalo**

Reid L W *The Elements of the Theory of Algebraic Numbers* 1910 Macmillan New York (This book also discusses fields and ideals)

Robinson A *Numbers and Ideals* **1965** **Holden** Day San Francisco

Stoll R R *Linear Algebra and Matrix Theory* 1952 McGraw Hill New York

Weisner L *Introduction to the Theory of Equations* 1938 Macmillan New York

Index